D10.10

Standardization Report (3)

Document Identification	
Date	26.11.2019
Status	Final
Version	Version 1.0

Related WP	10	**Related Deliverable(s)**	D 10.9
Lead Authors	F.-M. Kamm	**Dissemination Level**	PU
Lead Participants	G+D	**Contributors**	Atos, NLnetLabs, OIX, FhG, TUG
Reviewers	DTU, UPRC		

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 a continuously updated report, concentrating on the main activities and results within a certain reporting period.

For improved readability, chapters 4-7 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, Michael Lamla	G+D
Sue Dawes, Michelle Parkes	OIX
Martin Hoffmann	NLnetLabs
Sebastian Kurowski	FhG
Peter Lipp	TUG
Javier Cordero Presa	Atos
Javier Salazar Gomez	Correos

2.2 History

Version	Date	Author	Changes
0.1	28.10.2019	F.-M. Kamm	Initial version
0.2	06.11.2019	F.-M. Kamm	Partner contributions added
0.3	12.11.2019	F.-M. Kamm	Partner contributions added
0.4	21.11.2019	F.-M. Kamm	Partner contributions added
0.5	25.11.2019	F.-M. Kamm	Reviewer comments integrated
1.0	26.11.2019	F.-M. Kamm	Reviewer comments integrated

3. Table of Contents

3.1 Table of Acronyms

AdES	Advanced Electronic Signature
API	Application Programming Interface
ASiC	Associated Signature Container
B2B	Business to Business
CAdES	CMS Advanced Electronic Signature
CB	Certification Body
CC	Common Criteria
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Électrotechnique
CMS	Cryptographic Message Syntax
CSC	Cloud Signature Consortium
DANE	DNS-based Authentication of Named Entities
DNS	Domain Name System
DNSOP	DNS Operations
DNSSEC	Domain Name System Security Extensions
EC	European Commission
EDI	Electronic Data Interchange
eID	Electronic identity
eIDAS	electronic IDentification, Authentication and trust Services
EN	European Norm
eSE	Embedded Secure Element
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute
FAPI	Financial-grape API
FDIS	Final Draft International Standard
FIDO	Fast Identity Online
G+D	Giesecke+Devrient
GDPR	General Data Protection Regulation
GP	Global Platform
GSMA	GSM Alliance
ICC	Integrated Circuit Card
ICT	Information and Communication Technologies
IdM	Identity Management
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
iGov	International Government Assurance Profile
IoT	Internet of Things
IPR	Intellectual Property Rights
ISCI	International Security Certification Initiative
ISO	International Standards Organisation
ITSEF	IT Security Evaluation Facility
JHAS	JIL Hardware Attack Subgroup
JIL	Joint Interpretation Library
JSON	Java Script Object Notation
JTC	Joint Technical Committee
LoA	Level of Assurance
MNO	Mobile Network Operator
MODRNA	Mobile Operator Discovery, Registration & Authentication

OIX	Open Identity Exchange
PAdES	PDF Advanced Electronic Signature
PAdES-DTS	PAdES Document Time-stamp digital signatures
PDF	Portable Document Format
PKI	Public Key Infrastructure
PReM	Postal Registered Electronic Mail
RFC	Request for Comment
SC	Sub-Committee
S-MIME	Secure / Multipurpose Internet Mail Extensions
SoC	System on Chip
SOGIS	Senior Official Group Information Systems Security
TC	Technical Committee
TEE	Trusted Execution Environment
TLD	Top-Level Domain
TLS	Transport Layer Security
TS	Technical Specification
TSP	Trusted Service Provider
TUG	Technical University of Graz
UNCITRAL	United Nations Commission on International Trade Law
UNE	Asociación Española de Normalización
UPU	Universal Postal Union
WG	Working Group
XAdES	XML Advanced Electronic Signature
XML	Extended Markup Language

4. ISO/IEC JTC1

4.1 SC 17 WG 4

4.1.1 Scope of the working group

The official scope and title of JTC1/SC17/WG4 have 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.

The adopted scope is reflected by new standardization projects, started with "ICC-managed devices" or "Privacy-enhancing protocols and services". Current activities are focused on “mobile ID applications” using security devices outside of cards as secure elements within mobile devices.

4.1.2 Main achievements in year 3

The first of the new standards for enhancing mobile ID applications was started in 2018, named as "ISO/IEC 23220: Building blocks for identity management on mobile devices". A lot of new participants started in WG 4 to work on this standard, keeping it aligned with other current drafted standards, e.g. the mobile driving licence standards.

The content of the document increased significantly so that the standard was shifted to a series of standards consisting of 5 documents. Some of the documents are planned as a technical specification. The series of standards are now:

- Part 1: Generic system architectures and transaction flows of mobile eID-Systems
- Part 2: Data objects and encoding rules for generic eID-Systems
- Part 3: Protocols and services for issuing phase
- Part 4: Protocols and services for operational phase
- Part 5: Trust models and confidence level assessment

In parallel a new series of standards to facilitate the usage of a secure element in a mobile device for an app programmer has been established, named “ISO/IEC 23465: Programming interface for security devices”. The three-part-standard defines the architecture, the API and a proxy component to use the secure element within the mobile device by an app programmer without specific knowledge.

The established Chairman Advisory Subgroup reflecting the new topic of "Virtual ID" has provided, in the meanwhile, some working result but the work is still ongoing.

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 draft structure is a highly relevant document and an excellent fit for LIGHTest related topics since it has an own part on confidence levels (LoA), as they are used in LIGHTest mobile ID trust propagation. Therefore, the LIGHTest project was able to benefit from these discussions. 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 3

A 12-months 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 a 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, a stronger collaboration will be sought 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 standards, 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. The study period has concluded in the creation of a new work item. ISO/IEC 24391

will provide Guidelines for IoT-domotics security and privacy. Currently, the editing team of this new work item is being finalized, and liasions with SC25 WG1 are being approached.

WG4 is closely monitoring a new emerging standard, that is currently in its FDIS state. FDIS 22396 of TC 292 focuses on the resilience of communities and provides guidelines for the information exchange between organizations. This standard introduces a framework that comprises of the process of monitoring and review of information, leadership and commitment, analysis of context, design and implementation.

4.2.3 Impact on LIGHTest

A generic standard for the use and management of electronic trust service providers has not been established within SC27. Therefore, there are no expected deviations between the available standards and the LIGHTest components. As part of its ongoing standardization efforts, Fraunhofer will keep track of any standardization developments in the realm of electronic trust service providers and their compatibility to the LIGHTest components. ISO/IEC 24391 could include the LIGHTest trust language. Therefore these contributions may be introduced to the work item editors, once the editing team is finalized. Finally, the emerged FDIS 22396 of TC 292, which was not part of the LIGHTest standardization efforts, show that the assessment of various trust levels, especially the formal conceptualization and its automated assessment, along with the easy availability of trust lists, translation between trust lists, and the delegation of trust meet an increasing market demand. Hence, the standardization efforts show the increasing demand for LIGHTest and put a promising light on the future exploitation of the project outcomes.

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 by ETSI TC ESI during the lifetime of LIGHTest are:

- 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,
- EN 319 532-(1-4) Registered Electronic Delivery Services,
- EN 319 532-(1-4) Registered Electronic Mail Services,
- TS 119 122-3: CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES
- TS 119 142-3: PAdES digital signatures; Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS)
- TS 119 412: Cryptographic Suites
- EN 319 401: General Policy Requirements for Trust Service Providers
- TS 119 403 (1-3): Trust Service Provider Conformity Assessment
- EN 319 411-(1-3): Policy and security requirements for Trust Service Providers issuing certificates
- TS 119 412: Certificate Profiles
- 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.
- TS 119 443: Protocols for remote digital signature creation

5.1.2 Main achievements in year 3

The main topics ETSI TC ESI is currently working on include signature validation policies (TS 119 172), identity proofing, testing of latest new protocols for remote services like remote signature creation, validation and preservation, global acceptance of EU Trust Services, a schema for machine-readable cryptographic algorithm catalogues, conformity assessment of Trust Service Providers as well as JSON signatures. In the future, ETSI ESI will also be tackling digital signatures and quantum-safe crypto, the use of blockchains in trust services and deconflicting eIDAS and GDPR.

From Oct. 30th to Nov. 29th, ETSI holds a plug test on signature validation where more than 200 individuals representing more than 140 organisations will participate in. The aim is to check the interoperability of digital signatures and the validation capacities of the participants in order to help them detect possible issues which may lead to different validation results.

The interoperability testing will allow participants to test their digital signature validation tools and to cross-validate ETSI Electronic Signatures/Seals relying on EU Member States' Trusted Lists (based on TS 119 612 and TS 119 615, the latter under completion) and according to the following standards:

- European Standard EN 319 102-1 (Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation) and TS 119 102-1, meant to update in future EN 319 102-1
- TS 119 102-2 (Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report)
- TS 119 172-4 (Signature Validation Policy for European Qualified Electronic Signatures/Seals Using Trusted Lists, under completion)

The signature formats addressed in this event

- EN 319 132-1 and ETSI TS 103 171 for XAdES: XML Digital Signature
- EN 319 142-1 and ETSI TS 103 172 for PAdES: PDF Digital Signature
- EN 319 122-1 and ETSI TS 103 173 for CAdES: CMS Digital Signature
- EN 319 162-1 and ETSI TS 103 174 for ASiC: Associated Signature Container

TUG will be participating in this event.

5.1.3 Impact on LIGHTest

Most of the work done within ESI is relevant for LIGHTest since these standards, guides, and reports of ESI relate to electronic signatures and related trust infrastructures and LIGHTest aims at a global cross-domain trust infrastructure. eIDAS, which is a driving force within ETSI ESI, is also very relevant for the LIGHTest work, as can be seen from the pilots. Thus there is a lot of synergy of the work done in this project with the standardisation work from ETSI.

Two of the standards are especially relevant for LIGHTest: EN 319 102-1 and EN 319 102-2, Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation and Part 2: Signature Validation Report. TUG was the editor of these standards and the software that implement the signature validation procedures within LIGHTest is conformant to the procedures specified in 102-1. TUG will also be testing their validation implementation used in LIGHTest during the ETSI plug test as described above.

With TUG as an active partner in this group, a strong link to the LIGHTest project is given.

6. CEN / CENELEC

CEN, the European Committee for Standardization, is an association that brings together the National Standardization Bodies of 34 European countries. CEN provides a platform for the development of European Standards and other technical documents in relation to various kinds of products, materials, services and processes.

European Standardization plays an important role in the development of the European Single Market. The fact that each European Standard is recognized across the whole of Europe, and automatically becomes the national standard in 34 European countries, makes it much easier for businesses to sell their goods or services to customers throughout the European Single Market.

CEN supports standardization activities in relation to a wide range of fields and sectors including air and space, construction, consumer products, defense and security, energy, the environment, food and feed, health and safety, healthcare, ICT and Postal services.

The scope of the CEN/TC 331 includes the postal market which ranges from non-express letters to parcels including the extension to the digital services linked with the physical postal products or services.

The work of CEN/TC 331 is mainly focused on the interfaces between stakeholders in the postal value chain and various aspects of the measurement of quality of service. In addition, CEN/TC 331 works on hybrid mail, (automatic) identification and tracking of mail items, apertures in letter boxes, receptacles, address data, and forms.

6.1 TC 331 WG2 (Postal sector – New Digital Services)

6.1.1 Scope of the working group

This Working Group from CEN / CENELEC is focused on the new digital services, like the hybrid mail, including secured electronic postal services and postal registered email, the reverse hybrid mail, the electronic identity, while remaining within the competencies of the members of the different structures of CEN/TC 331.

The goals of the WG 2 are oriented to the support of the development of the new digital markets around the physical postal exchanges, including the interconnectivity to UPU postal supply chain management solutions. To afford wider postal sector stakeholders access to these solutions, to foster electronic data exchanges with designated operators via standard UPU electronic data interchange (EDI) messages, and also to allow these stakeholders to assist in raising and resolving anomalies in the postal supply chain.

6.1.2 Main achievements in year 3

As national observers within this working group, Javier Salazar and Carlos Balot, team members of the Correos pilot, attended several private meetings at the offices of UNE, the Spanish standardization body that interacts with CEN / CENELEC. As CEN / CENELEC national observers for Postal Services Standardization specialized in Digital Services (TC331 WG2), they had the chance to explain and discuss the possibilities of LIGHTest at an international standardization level.

Regarding CEN / CENELEC, as national observers, they are part of every European standardization done for trust digital services and its business applicability. As well as with UPU, this directly impacts the use and sustainability of LIGHTest at the business level.

6.1.3 Impact on LIGHTest

Several standards that have been or are developed within CEN / CENELEC and ISO are relevant for using LIGHTest mechanisms in trust decisions. LIGHTest needs to be aware of any requirements when using standard technologies. Feedback from this standardization group has been fed back into the LIGHTest project to consider a real-world use case, as addressed by the Correos pilot.

7. Alliances/Industry

7.1 FIDO Security WG

7.1.1 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.

7.1.2 Main achievements in year 3

The FIDO WG has been renamed to “FIDO Security & Privacy Requirements Working Group” to better reflect the privacy-related work of FIDO in general and of this WG. By design, the FIDO protocol is already privacy-friendly but in conjunction with the security levels which determine the actual level of protection of the user credentials, the practically achievable privacy level and security level are strongly correlated. The definition of FIDO security levels that has already started two years ago has continued and is now much more advanced than in the previous year. A whitepaper on security levels has been published by the alliance, documenting parts of this work.

While the entry security levels as well as the highest levels are already well defined, there is still some discussion ongoing regarding the medium levels. Especially the mapping of Global Platform (GP) conformant Trusted Execution Environments (TEEs) to the FIDO levels is still under discussion. Currently, it is debated whether a GP TEE should be mapped to level L2+ or level 3. On top of the definition of classical FIDO security levels there has also been some progress on defining biometric security levels for the pure biometric certification of FIDO components. First commercial components on off-the-shelf mobile devices have now been certified according to this scheme.

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.

7.1.3 Impact on LIGHTest

The FIDO protocol and the work of the FIDO alliance are 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. With the progress made over the last years the mapping picture is now becoming more and more clear. Therefore, it has been 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. The LIGHTest mobile ID demonstrator contains an example of how the mapping of a FIDO authenticator (identified by the integrated attestation scheme) to a mobile ID LoA can be done by leveraging the LIGHTest infrastructure for querying this information within the trust domain.

7.2 JHAS

7.2.1 Scope of the working group

JHAS is the Joint Interpretation Library (JIL) Hardware related Attacks Subgroup The Joint Interpretation Library (JIL) is a European working group steered by the SOGIS group (https://www.sogis.eu/) 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 (Embedded Secure Elements (eSE), System on Chip (SoC) e.g.) 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” (https://www.sogis.eu/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v3-0.pdf).

7.2.2 Main achievements in year 3

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.

Very intensive discussion about open samples took place in two subgroup meetings. Representatives from schemes, labs and vendors discussed very openly and fruitfully the usage of open samples in the evaluation process.

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

- 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.
- Tools: output is an updated table of tools in JHAS document JIL-Application-of-Attack-Potential-to-Smartcards to clarify the border between standard, specialized and bespoken equipment.
- Terms of reference: output is a document which includes updated objectives, organization, membership and rules of JHAS.

7.2.3 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 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 HW-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. The work in JHAS is directly linked to the practical definition of the more theoretical Common Criteria (CC) attack potential definitions. In the eIDAS trust scheme, these attack potential levels are directly mapped to the eIDAS levels. Therefore, this work is directly relevant for the LoA determination within the eIDAS trust scheme, especially for the use of HW-based security to store the LIGHTest mobile ID credentials.

7.3 GSMA Mobile Connect

7.3.1 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.

7.3.2 Main achievements in year 3

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 7.5 for more information on engagement with OpenID and the MODRNA working group). Over year 3 the contact with GSMA representatives has continued as a member of the OpenID Foundation and an adopting organization of the OpenID Connect Standard.

7.3.3 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.

7.4 Cloud Signature Consortium

7.4.1 Scope of the working group

The Cloud Signature Consortium is 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.

The CSC has formed a technical committee to focus on furthering the technical aspects of trust service development, testing, communication and adaptation. It collects and coordinates the technical interests of CSC Members when it comes to trust services for electronic transactions, monitors the latest technical developments, recommends the priorities, objectives and milestones to the board and ensures compliance with relevant international, EU and national regulations. It also plans and oversees technical activities including but not limited to: research, meetings, prototyping, testing, specifications development, publications, quality control, technical support, liaison with other technical stakeholders – to implement the agreed priorities, strategy, objectives and milestones for the technical development of e-trust services.

TUG is a member of the CSC and represented in the technical committee.

7.4.2 Main achievements in year 3

The consortium has released V1.0.4.0 API specification for Remote Electronic Signatures and Remote Electronic Seals, the updated version of the V1 API technical specification with new IPR information and errata, a standard for a signature creation API, based on web-services and JSON, which provides an interface allowing applications to access remote signature creation services, and is actively working on implementing these specifications. Work on signature validation service specification has been put on hold but will be worked on in the future.

7.4.3 Impact on LIGHTest

An informal liaison with the Cloud Signature Consortium helps the success of LIGHTest by informing relevant partners within the CSC about the ideas and work done within LIGHTest. It also allows ensuring that future technical developments remain compatible in the sense that a CSC specification does not make use of LIGHTest technology in the future difficult or even impossible. With TUG as an active partner in this group a strong link to the LIGHTest project is given.

7.5 OpenID Connect

7.5.1 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.

OpenID Connect continues to have significant adoption with millions of OpenID transactions taking place on a daily basis. The most recent and significant implementation of OpenID Connect is with Sign-in with Apple. Additionally, Connect profiles such as the Financial-grade API (FAPI) and Mobile Operator Discovery, Registration & autheNticAtion (MORDNA) are helping drive global open banking and mobile ecosystems and solutions. The significant adoption of the OpenID Certification Program further enhances the robustness of Connect and associated profiles by allowing self-certification of implementations to ensure conformance to the standards.

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 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.

7.5.2 Main achievements in year 3

The consortium partner, Open Identity Exchange (OIX) has continued to provide updates to OpenID Foundation Board meetings, executive committee meetings and most of the quarterly OpenID Foundation workshops.

All groups are keeping an eye on LIGHTest and it's a constant on-going topic of conversation on the agenda. The OpenID Foundation chairs and participants continue to monitor the LIGHTest project and its outputs and look forward to seeing the end results which will form on-going discussions in the future.

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 MODRNA working group, which will allow for engagement on the LIGHTest standardisation working package.

7.5.3 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.

7.6 IETF

7.6.1 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.

7.6.2 Main achievements in year 3

After starting the standardization work at the IETF's DNSOP working group it was postponed in year 2 because of ongoing dependent work in the group. This work was finished in March 2019 and culminated in the publication of RFC 8552, 'Scoped Interpretation of DNS Resource Records through "Underscored" Naming of Attribute Leaves.' This RFC provides a foundation and guidance for standardization of the DNS usage of LIGHTest.

NLNET engaged with the community in exploring a way forward and is currently writing an Internet Draft that will be submitted to the DNSOP working group towards the end of the year. NLNET will continue to pursue this work beyond the end of the LIGHTest project.

7.6.3 Impact on LIGHTest

Standardization work with the IETF is important for wide acceptance and deployment of LIGHTest as the DNS will be an integral part of the LIGHTest framework. In addition, the DNS community in the IETF has provided valuable feedback regarding the architecture of the infrastructure and its security and reliability considerations. With the work of NLNET continuing even after the end of the LIGHTest project, it can be expected that the integration and promotion of LIGHTest will be deepened even further beyond the initial level that was partly hindered by the lack of maturity in the early part of the LIGHTest project.

7.7 Universal Postal Union

7.7.1 Scope of the 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 the 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 access/use costs associated for all external entities.

7.7.2 Main achievements in year 3

The consortium partner, Correos has continued to provide updates on the standards and the activities of the UPU that might be of interest for the LIGHTest project, as Correos is an active member of 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 evaluated during the design of the demonstrator use cases as part of the implementation phase of the LIGHTest platform.

7.7.3 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 bring the latest top-level domain definitions 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.

7.8 .post

7.8.1 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.

7.8.2 Main achievements in year 3

During the third year of the project, the main focus was 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. While the design and implementation phase was in progress, this mutual collaboration has been evaluated.

Víctor Martín, as Deputy Director of Digital Business in Correos, participated remotely in several private meetings as part of the workshops of the Steering Committee follow-up meetings of UN UPU (Universal Postal Union) .post during 2019, getting the chances and opportunities to explain and explore synergies of the LIGHTest Project with all .post initiatives.

As a matter of interest to UPU, the .post project empowers a specific TLD for the postal sector. This obviously has important synergies with LIGHTest project, as DNS is the pillar for TLDs and trust based on DNSs could simplify the digital trust services that the postal sector is already providing.

7.8.3 Impact on LIGHTest

Given that .post is 100% secured by DNSSEC, in case of UPU the goal is to re-use any LIGHTest results by UPU in order to bring the latest top-level domain definitions 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 (TLS) 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 exists no 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 based on taste. If they are to be used, a domain name for where these records will be placed needs to be specified and standardized. 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.

7.9 UNCITRAL Expert Group

7.9.1 Scope of the working group

The UNCITRAL secretariat organized an expert group meeting to consult on draft provisions on the cross-border recognition of identity management (IdM) and trust services, which the Secretariat is preparing for the consideration of UNCITRAL Working Group IV (Electronic Commerce) at its fifty-ninth session, to be held in November 2019. The expert group meeting took place at the Vienna International Centre (Vienna, Austria) on 22-23 July 2019.

7.9.2 Main achievemets in year 3

During the expert group meeting, the LIGHTest unified model for trust schemes was presented and received very high interest from all participants. It could provide the basis for one of the most urgent challenges for cross-border recognition of trust schemes as it allows to make detailed comparisons between different trust schemes and their levels of assurance. The expert group made the recommendation to make use of this model to the UNCITRAL Working Group IV.

7.9.3 Impact on LIGHTest

This activity was mainly opportunity-driven and came up during project year 3. It has turned out to be an excellent platform to present the core capabilities of LIGHTest to a relevant global community, since LIGHTest can offer some key features for the cross-border use case which are of real interest for the group. It may therefore turn out to be one of the possible exploitation opportunities for LIGHTest even after the end of the project.

8. Summary /Conclusions

As shown in the last chapters (4-7), 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 third year has seen further progress on intensifying the relations between LIGHTest and some relevant standardization groups. 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, and new groups like CEN/CENELEC and UNCITRAL have been added. This has created additional visibility of LIGHTest in the standardization community. Since it is important to present mature and concrete concepts/results, some of the early activities have proven to be too early to generate sufficient interest in LIGHTest. However, towards the end of the project this interest has constantly increased and it can be expected that even beyond the lifetime of the LIGHTest project these concepts will be further communicated to and discussed with the relevant standardization groups.

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 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/ES), 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.