LIGHT*est* -- A Lightweight Infrastructure for Global Heterogeneous Trust Management

Bud P. Bruegger[1], Peter Lipp[2]

Abstract: LIGHT*est* is a project that is partially funded by the European Commission as an Innovation Action as part of the Horizon2020 program under grant agreement number 700321. LIGHT*est*'s objective is to create a **L**ightweight **I**nfrastructure for **G**lobal **H**eterogeneous **T**rust management in support of an open **E**cosystem of **S**takeholders and **T**rust schemes. We show supported scenarios, motivate the necessity for global trust management and discuss related work. Then we present how LIGHT*est* addresses the challenges of global trust management, its reference architecture and the pilot applications.

Keywords: trust management, trust decisions, trusted lists, global trust infrastructure

1 On Trust and Trust Decisions

There are many possible definitions of trust [Gefen]. In LIGHT*est*, a trust decision determines whether a verifier should act on an electronically received transaction. This is illustrated in Figure 1a.

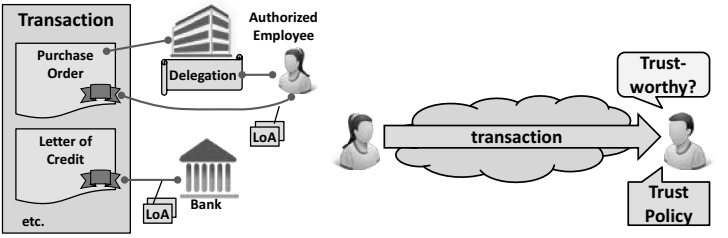

Figure 1: (a) The evaluation of trustworthiness of a transaction based on a trust policy, and (b) a prototypical transaction consisting of multiple parts and involving delegation.

A trust decision depends on the verifier's perception of risk, i.e. the probability and extent of possible damage and the availability of mitigation measures such as legal enforceability or insurance. This can be expressed in the verifier's trust policy.

Since verifiers often lack direct acquaintance of the partners involved in the transaction, they rely on authorities asserting their electronic identities as well as other trust-relevant

[1] Fraunhofer IAO, Identity Management, Nobelstr. 12, 70569 Stuttgart, bud.bruegger@iao.fraunhofer.de
[2] Technische Universität Graz, Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie, Inffeldgasse 16a, 8010 Graz, peter.lipp@iaik.tugraz.at

properties. These authorities manage *trust schemes* that assign Levels of Assurance (LoAs) to identities. Scheme information can, for example, be published in the form of a *Trusted List* (or Trust Status List) as defined, for example, by ETSI [ETSI16].

Figure 1b shows, by example of electronic trade, how a transaction involves multiple data records, each of them being associated with some identity[3]. For example, the purchase order in the figure is associated with the authorized employee who signed it; the letter of credit is associated with its issuing bank. The association can be either direct or indirect through a mechanism of delegation [Mod05] [Van09] [Eur09] [STO] [Lei14].

Trust in transaction data is derived from the LoA of the identities that are linked to the various records. The LoA of a single identity can be rated differently by different authorities issuing trust lists. It is important for a globally scalable trust infrastructure such as LIGHT^{est} that multiple, potentially conflicting perceptions of trust can co-exist and avoiding the need for all verifiers to share a single perception in order to participate.

It is up to verifiers to determine in their trust policies which trust schemes (lists) are to be applied. The trust policy also states the minimal levels of assurance required for each data record in order to consider the transaction trustworthy.

1.1 Different Trust Schemes for Different Aspects of Trust

Many real-world applications require a variety of trust schemes, focusing on different aspects of trust influencing the transaction risks. Examples include:

- **Identity-centric**: This type of trust, also addressed by eIDAS [eIDAS], focuses on the certainty that an electronic entity represents a certain legal entity. This identity-centric type of trust is the basis for legal validity and enforcement.
- **Reputation-centric:** This includes properties such as customer satisfaction ratings in “electronic shopping”.
- **Business-centric**: This includes properties such as credit ratings, the capital that is backing liability, etc. Business-centric ratings are often specific to a business area and/or a type of transaction.
- **Quality-centric**: This includes ratings of the quality of offered merchandize or services that is verified and certified by some authority.
- **Compliance-centric**: Compliance-centric trust schemes typically use Boolean levels of assurance (compliant/non-compliant) and include things such as compliance with regulations on the protection of personal data, compliance with export regulations, or the Italian anti-mafia certification.
- **Based on direct experience**: A trust scheme may also be based on direct experience with the transaction participants and could, for example, be expressed in the form of black- and whitelists.

[3] Such an association can, for example, be established by electronic signatures.

1.2 Types of Trust Schemes

To cater to different requirements of trust management, LIGHT*est* supports a variety of different trust scheme types. They include the following: **(i) Boolean** trust schemes, for example indicating whether an issuer is **qualified**, **(ii)** Trust schemes using **levels of assurance** and **(iii)** Trust schemes certifying **arbitrary sets of attributes**.

While most common trust schemes and the data certified will be public, LIGHT*est* technology can also be used for certifying potentially sensitive data through the use of **sensitive trust schemes**. They avoid linkability to the entities it describes and optionally supports selective disclosure of attributes under the control of these entities.

2 Previous and Related Work

LIGHT*est* can be seen as an extension and evolution of the trust infrastructure of the now completed FP7 project *FutureID* [Fut][Bru15]. The following shows how LIGHT*est* advances the state of the art:

2.1 Trust Lists

Probably the most common way to express trust schemes is in the form of signed trust lists. Among the best known are ETSI's TS 119 612 [ETSI16] with its update that is expected as basis for an eIDAS implementation act and SAML V2.0 Identity Assurance Profiles [SAML10] used, for example, by the Kantara initiative [Kan].

The direct use of trust lists by verifiers is very onerous. It is comparable to the direct use of certificate revocation lists that have been largely replaced by OCSP [RFC6960] providing a way to use simple queries of the status of individual certificates.

To use trust lists directly, verifiers are responsible for the following tasks: **(i)** Securely provision the list's trust anchor (the certificate used to validate the list's signature) and location, **(ii)** download the list, **(iii)** verify the list's signature, **(iv)** parse the list, **(v)** load the list data in some local storage that permits querying of individual entries, **(vi)** repeat some of the above tasks every time the list is updated or its trust anchor expires and has to be renewed. Since such a procedure is too cumbersome for normal verifiers, this complexity and responsibility will typically be offloaded to Validation Authorities.

LIGHT*est* provides an alternative solution to Validation Authorities that is conceptually equivalent to that of OCSP: It enables verifiers to query individual trust list entries over the network at the authority who issued the trust list[4].

Figure 2 illustrates the difference between the direct use of trust lists by verifiers and the

[4] Or a trusted third party who publishes the trust list in representation of this authority.

much more convenient querying of trust list items through the LIGHT*est* trust infrastructure. It shows how the verification of the trustworthiness of a single certificate is managed in the two cases.

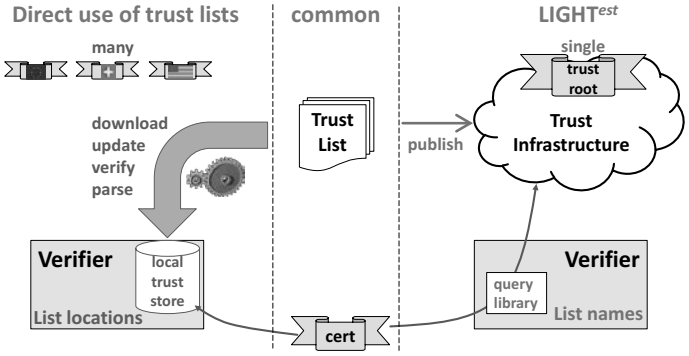

Figure 2: Comparison of direct use of a trust lists vs. the querying of a list item in LIGHT*est*.

The following advantages of the LIGHT*est* approach are evident: A single trust root covers all current and future trust lists in LIGHT*est*, while verifiers need to provision and update one trust anchor per list in case of direct use. LIGHT*est* replaces the cumbersome tasks or setting up and continuously updating a local trust store with simple queries of list items.

2.2 Validation Authorities

Validation authorities (VAs) relieve verifiers from the burdensome management of trust lists. Prime examples are the VAs operated by member states for qualified signatures. Figure 3 illustrates how a VA interfaces between verifiers and trust lists, offering a query interface. Evidently, all verifiers share the same perception of trust.

Figure 4 shows the alternative approach taken by LIGHT*est*. Here, every trust list is rendered queryable through its publication in the LIGHT*est* trust infrastructure. Shifting the point of publication to the trust lists allows different verifiers to apply different perceptions of trust, i.e., different sets of trust lists.

Another difference between validation authorities and LIGHT*est* is also illustrated in these figures: In LIGHT*est*, verifiers send queries that are very small, typically a single network packet[5], containing only a hash of the certificate to verify.

The LIGHT*est* approach is thus by several orders of magnitude more efficient in the required network resources and the possible response times. When planning for global scalability, such efficiency becomes important.

[5] DNS queries preferentially use a single UDP packet.

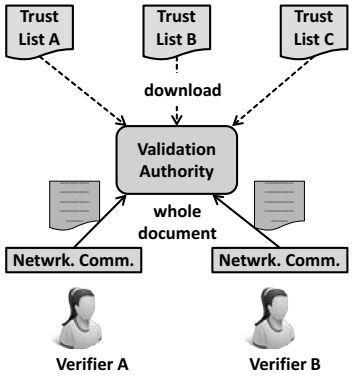

Figure 3: Validation authorities as interface between verifiers and trust lists.

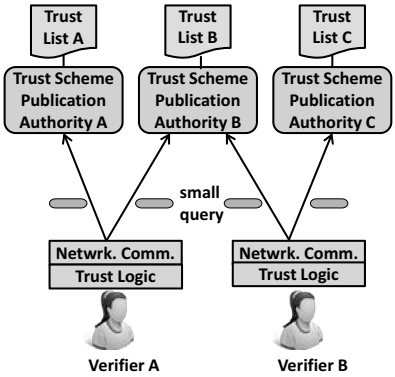

Figure 4: Different verifiers use different combinations of trust schemes as defined in their trust policy.

In many application areas, confidentiality and privacy may be a bigger issue than efficiency. For example, in the field of e-procurement, neither purchaser nor supplier may be willing to send the full data to a validation authority operated by a national authority. Since LIGHT*est* offers the same convenience to verifiers as VAs without requiring access to signed documents, its range of application is much wider.

LIGHT*est* avoids introducing intermediaries such that every involved stakeholder is directly responsible for the data it publishes. It is therefore better suited for cross-jurisdiction settings.

3 The European LIGHT*est* Project

LIGHT*est* is a project that is partially funded by the European Commission as an Innovation Action as part of the Horizon2020 program under grant agreement number 700321. Its start date is September 1, 2016 and its duration 36 months. The estimated project cost is 8.7 Mio Euros.

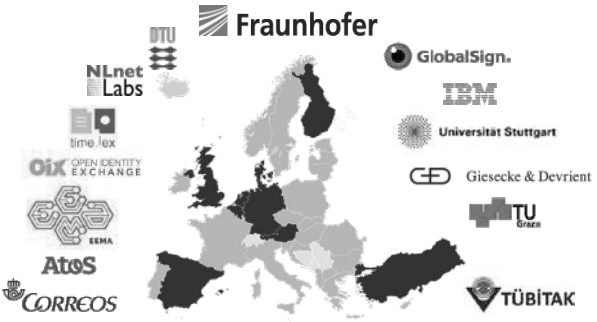

Figure 5: The LIGHT*est* consortium.

The LIGHT*est* consortium is consists of 14 partners from 9 countries, namely Austria, Belgium, Denmark, Finland, Germany, Spain, The Netherlands, Turkey, and the United Kingdom. The project is coordinated by Fraunhofer. The partners are shown in Figure 5.

Our objective is to build a global infrastructure. For this reason, the consortium of the EC-funded project includes the European branches of organizations that operate globally, namely the Open Identity Exchange and GlobalSign, IBM, and G&D. Further outreach beyond Europe will be implemented through the composition of the advisory board and the associate partner program.

4 How LIGHT*est* Addresses Challenges of Global Trust Management

The following describes some major challenges of global trust management and how LIGHT*est* addresses them.

4.1 Creation of a Global Trust Infrastructure at Feasible Effort

The effort required to create a global infrastructure is enormous and in most cases well out of reach of an EC-funded project with a very limited budget. This becomes even more evident when considering some of the requirements of the infrastructure: **(i)** Global agreement on the governance of the single trust root. **(ii)** Global organization to register unique names of trust schemes. **(iii)** A highly available and efficient global infrastructure for scheme location and queries. **(iv)** Design of the necessary protocols and their international standardization. **(v)** Development and maturation of software implementations of these protocols. **(vi)** Detailed security analysis of the infrastructure and of specific software products. **(vii)** Registration of trust schemes at the global registry. **(viii)** Training of staff to operate servers that publish trust schemes.

LIGHT*est* addresses this possibly most difficult challenge through reuse of the existing Domain Name System (DNS. In particular, LIGHT*est* employs the global DNS system as-is. Only marginal additions render it usable as a global trust infrastructure. It does so by following well-established strategies of other kinds of trust management[6].

4.2 Global Acceptance of the Approach Beyond Europe

A trust infrastructure that is global in a technical sense is only useful if it is actually accepted by at least the majority of stakeholders. Such a trust infrastructure needs to

[6] Namely, LIGHT*est* adds to an existing family of trust management approaches in the family of IETF RFCs around DANE (DNS-based Authentication of Named Entities).

support global interoperability of trust schemes and trust queries.

LIGHT*est* addresses this challenge by embedding its technical innovations into an inclusive and collaborative strategy that positions LIGHT*est* from the start as a global initiative, open to extra-European collaboration.

4.3 Support for Heterogeneous Trust Models, since Homogeneous Models Fail to Scale Globally

Most current approaches assume that all participants share a single homogeneous perception of trust. Prime examples are "circles of trust". In a global setting, this assumption fails to apply. A global infrastructure therefore has to support heterogeneous trust models where stakeholders without a common perception of trust can collaborate.

LIGHT*est* supports heterogeneous models of trust by moving the decision point for who is trusted to the verifier's trust policy. It typically selects and combines few existing large scale trust schemes (such as that of EU qualified signature) and can further personalize it with local black- and white-lists.

4.4 Automatic Handling of Subsidiarity Principle in Trust Schemes

Many existing trust schemes are constructed based on the subsidiarity principle. A global trust infrastructure must support such schemes automatically and transparent to verifiers. An example for this is the trust scheme of European qualified signatures where the European Commission uses a "*list of lists*" to delegate national portions of this trust scheme to the *trusted lists* created by Member States. While it may be easy to define hierarchical trust schemes, the challenge is to make it easy for verifiers to seamlessly follow all delegations to lower hierarchical nodes.

LIGHT*est* addresses this challenge by using the native and massively proven DNS mechanism to delegate the management of sub-domains to third parties. The mechanism can support an arbitrary depth of the hierarchy and the LIGHT*est* client libraries render the hierarchical structure of trust schemes transparent to verifiers.

4.5 Access to Trust Schemes based on Human-Readable Names

To enable non-technical decision makers understanding and authoring their trust policies, trust schemes must have globally unique but human-readable names. Accessing trust scheme data solely based on this name avoids error-prone configuration and removes significant vectors of attack. Enterprises operating on a global market have to accept signatures from customers world-wide and thus deal with a large number of trust schemes.

Technically, the use of current trust schemes typically requires two elements: **(i)** The location from where some trust list can be downloaded and **(ii)** the certificate that has signed the trust list and is required for verification.

A manual assignment of names to location/certificate pairs during configuration of a system is highly cumbersome and error prone. A global trust infrastructure should therefore render it possible to identify trust schemes with simple names suited for use by non-technical decision makers who define the organization's trust policy. These names should directly be usable to technically access and verify the actual data of the corresponding trust scheme.

LIGHT*est* addresses this challenge by using DNS domain names to identify trust schemes. For example, the European trust scheme of qualified signatures may be named "*qualified.TRUST.ec.eu*". Here, *qualified* is the scheme name, *ec.eu* the authority responsible for the scheme, and *TRUST* a standardized constant word used across the trust infrastructure. Using the existing DNS, this name can then be used by software to locate and access the data that is contained in the named trust scheme.

4.6 Use of a Single Trust Root to Replace a Multitude of trust Anchors

On a global market, automatic verification of trust requires that the certificates of all trusted scheme operators issuing trusted lists must be loaded into the configuration of the system. These certificates are required to validate that the content of the trust scheme (list[7]) originates from a trusted source and not from some hostile attacker.

Provisioning such trust anchors is a highly security sensitive task and an attractive attack vector. An easy solution is the use of a single trust root from which all trust is derived.

LIGHT*est* addresses this challenge by applying the existing, unique, and globally accepted trust root of the DNS. The standard mechanism of the DNS (with DNSSEC extension) allows to derive trust in trust scheme data from this single trust root and the (domain) name of the trust scheme.

4.7 Integration of Multiple Types of Trust Schemes in a Single Infrastructure

Real world trust decisions on electronic transactions typically require taking several different aspects of trust into account. A global trust infrastructure must be able to support all these aspects to avoid that verifiers need to access many different trust infrastructures and manage interoperability issues.

For example, to validate a purchase order with attached letter of credit, the following trust aspects may be involved: **(i)** Are the seals of the purchaser and bank qualified and

[7] While a "list" is mentioned here, the same reasoning applies also to possible Validation Authorities.

thus legally valid? **(ii)** Is the capitalization of the purchaser sufficient for the total amount of the order? **(iii)** Is the bank who issued the letter of credit trusted for the amount guaranteed?

The example illustrates that this involves different authorities using different trust schemes with different levels of assurance. It is evident that requiring multiple trust infrastructures would make validation very difficult and complex and multiply the cost as well. We therefore believe that the only viable way to enable electronic transactions on the single market is the conception of a single trust infrastructure that can support arbitrary current and future trust schemes.

LIGHTest addresses this challenge by using a very generic model of trust scheme and supporting an open number of trust schemes to coexist concurrently.

5 The LIGHT*est* Reference Architecture

Figure 6 shows the LIGHT*est* reference architecture with all the major software components. It illustrates how a verifier can validate a received electronic transaction based on her individual trust policy and queries to the LIGHT*est* reference trust infrastructure.

Verifiers use Policy Authoring and Visualization Tools to state their individual trust policy. These tools support non-technical decision makers understanding and creating trust policies that can be applied by the Automatic Trust Verifier component (ATV).

In a cross-jurisdiction setting, different trust schemes are used to describe conceptually equivalent aspects. To make it easy to verifiers, Trust Translation Authorities (TTAs), provide the necessary translation data to map the levels of assurance of the foreign trust scheme to its equivalent in the domestic trust scheme. For example, an American authentication security of Level 3 could be mapped to the eIDAS level *substantial*.

Very often, data records that compose an electronic transaction are not directly signed by the legal entity responsible for it (e.g., using a company seal), but by a natural person that acts as an authorized representative for the former based on a delegation. The architecture therefore foresees the component of Delegation Publishers (DPs) that permit verifiers to query delegations and mandates.

All server components are implemented as DNS name servers. Organizations intended to publish trust schemes, translations schemes, and/or delegations can reuse their existing DNS servers (with security extension) or the existing outsourcing of this functionality.

In the same way as the DANE (DNS-based Authentication of Named Entities) standard [rfc7671] uses the DNS security extension to derive trust in TLS server certificates, LIGHT*est* derives trust in trust scheme, translation, and delegation data. Chains of trust

can be stored as receipts that can be validated at a later point in time.

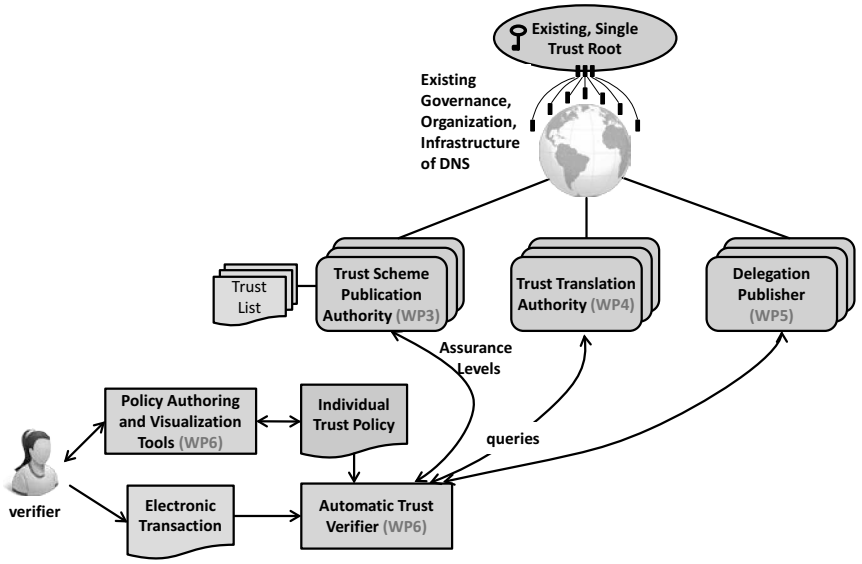

Figure 6: The LIGHT^{est} Reference Architecture.

6 The LIGHT^{est} Pilot Applications

Two pilots to demonstrate LIGHT^{est} in an operational environment. They demonstrate the ease of integration of LIGHT^{est} components in existing systems and the benefits provided by the LIGHT^{est} functionality in real world usage scenarios.

One pilot uses LIGHT^{est} for all trust management in the cloud-based e-Correos platform that provides trustworthy communication services to citizens and businesses at a national scale. The other pilot focuses on e-invoicing in the OpenPePPOL [Ope]environment to establish trust in the various signatories and demonstrate the delegation-enabling of applications through LIGHT^{est}.

7 The LIGHT^{est} Approach for Going Global

To achieve acceptance also beyond Europe, as is necessary for a truly global trust infrastructure, LIGHT^{est} uses an open and inclusive process that involves as much as possible also non-European stakeholders:

(i) LIGHT^{est} considers also extra-European existing schemes in its inventories and attempts to assess also the requirements of non-European stakeholders. **(ii)** LIGHT^{est}

encourages participation of non-European stakeholders through global players in the consortium, the advisory board, and an associate partner program. **(iii)** LIGHT*est* attempts international standardization of key elements, for example in the IETF. This process is by definition open to stakeholders world-wide. **(iv)** All DNS-related key components of LIGHT*est* will be open source. The developed code will be hosted on an existing project portal such as Joinup, inviting contributions from outside the project from the beginning.

To support building up a global community, LIGHT*est* applies a community-based dissemination strategy. For this purpose, a community is built around a vision of *universal, global, and interoperable trust management through the single standard solution offered by LIGHTest.* This vision can be shared by stakeholders with different and potentially competing economic interests and is supported by the fact that the growth of the community in support of this vision will benefit every single member.

To achieve the above objectives, communication activities are integrated in a systematic strategy of community building. The big difference between community-based, and the "standard" dissemination strategies of projects lies in the amplification factor. In "standard" dissemination, the effort is carried solely by the project partners and is therefore necessarily limited, for example compared to global ambitions. In contrast, a community-based approach empowers project-external community members to disseminate the community's vision independently of the project and without funding through the project. In the ideal case, a vision can "go viral". This approach can adapt the dissemination to local languages and cultural settings, exploit opportunities that project partners could not possibly know about, and can access additional funding sources and support in other parts of the world.

8 Conclusions

This paper has described the major characteristics of the EC-funded LIGHT*est* project. It promises a high impact through its wide range of applicability, its flexible support for a variety of trust schemes and trust aspects, and its global design both technically and through its planned community. The far-reaching use of the existing, globally implemented domain name system makes a global roll out at all possible. The use of the single trust root of the DNS is a key for real-world usability of the infrastructure.

While the partial funding by the European Commission is limited to its Consortium, LIGHT*est* plans to build up a global community that promotes the implementation of the global trust infrastructure well beyond Europe. International standardization and the planned availability of open source implementations of all necessary components facilitates large-scale uptake.

The LIGHT*est* project invites all interested parties, including non-European stakeholders, to participate in various ways in the project. Possibilities include contribution of one's

trust schemes to the inventory of the project to ascertain its support in the produced standards and software, serving on the advisory board to represent regional or sectorial requirements, participation in standardization, promoting and disseminating the vision of LIGHT^{est} , and setting up of additional demonstrators and pilots. Interested parties are asked to contact the authors.

9 References

[Bru15] Bruegger B.P. (2015): The Globally Scalable FutureID Trust Infrastructure. Marseille, France.

[eIDAS] EUROPEAN PARLIAMENT AND OF THE COUNCIL (2014): *electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*., DOI 2014/910/EU.

[ETSI16] ETSI (2016): *TS 119 612: Electronic Signatures and Infrastructures (ESI); Trusted Lists.* http://www.etsi.org/deliver/etsi_ts/119600_119699/119612 /02.02.01_60/ ts_119612v020201p.pdf,

[Eur09] European Commission (2009): *Study on eID Interoperability for PEGS: Update of Country Profiles*. IDABC Programme.

[Fut] *FutureID*. http://FutureID.eu,

[Gefen] Gefen ; Rao V.S. und Tractinsky (2002): The Conceptualization of Trust, Risk and Their Relationship in Electronic Commerce: The Need for Clarification. In: *36th Hawaii International Conference on System Sciences (HICSS'03)*. Big Island, HI, USA: IEEE. S. 1-10.

[Kan] *Kantara*. https://kantarainitiative.org/trust-registry/ktr-trust-validation/,

[Lei14] Leitold H.; Lioy A. und Ribeiro (2014): STORK 2.0: Breaking New Grounds on eID and Mandates. Mesago Messe Frankfurt GmbH. S. 1-8.

[Mod05] Modinis study on identity management in eGovernment (2005): *Common Terminological Framework for Interoperable*. https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf,

[OASISDSS] OASIS: *Digital Signature Services*. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss,

[Ope] *OpenPEPPOL*. http://www.peppol.eu/,

[RFC2560] *RFC2560*. https://www.ietf.org/rfc/rfc2560.txt,

[SAML10] OASIS: *SAML Assurance Profile*. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.html,

[STO] STORK 2.0: *D2.1: Existing e-ID infrastructure analysis*. (Delivarable).

[Van09] Van Alsenoy ; De Cock ; Simoens K. et al. (2009): Delegation and digital mandates: Legal requirements and security objectives. *Computer Law & Security Review*, 25 (5). S. 415-432.