Heiko Roßnagel, Sven Wagner

LIGHTest

eine leichtgewichtige Infrastruktur für globales und heterogenes Vertrauensmanagement

Das von der EU-geförderte Forschungsprojekt LIGHTest entwickelt eine globale Vertrauensinfrastruktur, die es ermöglicht elektronische Transaktionen einfach und effizient zu verifizieren. Dabei baut LIGHTest auf der bereits verfügbaren Domain Name Service (DNS)-Infrastruktur auf. Dadurch ermöglicht es LIGHTest, die Vertrauenswürdigkeit von Transaktionen zu bewerten, auch wenn die beteiligten Instanzen unterschiedlichen Trust Domains angehören.

1 Einleitung

Da man seine Geschäftspartner früher oft persönlich kannte, waren Identitätserschleichung und Betrug eher selten. Heute sind elektronische Transaktionen jedoch ein integraler Bestandteil des täglichen Berufs- und Privatlebens. Daher ist es wichtig zu wissen, wer der Geschäftspartner auf der anderen Seite ist und ob dieser vertrauenswürdig ist. Dafür wird eine Zertifizierung von vertrauenswürdigen Identitäten benötigt. Diese Zertifizierungs-Infrastruktur ist in der EU bereits seit Jahren vorhanden. Allerdings ist es bei der Bewertung der Vertrauenswürdigkeit elektronischer Transaktionen immer noch recht mühsam, alle benötigten relevanten Informationen von den unterschiedlichen beteiligten Parteien zusammenzutragen. Dies stellt sich insbesondere dann besonders kompliziert dar, wenn mehr als eine *Trust Domain* involviert ist. Hier fehlt ein allgemeiner globaler Standard zur Veröffentlichung und Abfrage von Vertrauensinformationen. Ohne diesen Standard müssen während des Verifikationsprozesses zahlreiche unterschiedliche Protokolle und Formate abgefragt und ausgewertet werden.

Das EU-Projekt LIGHTest (*https://www.lightest.eu/*) versucht mit dem Aufbau einer globalen Vertrauensinfrastruktur dieses Problem zu lösen. LIGHTest nutzt dazu das *Domain Name System* (DNS) mit seiner bereits etablierten globalen Infrastruktur und Organisation sowie Kontrollstrukturen und Sicherheitsstandards. LIGHTest bietet unterschiedlichen Parteien die Möglichkeit ihre *Trust*-Informationen zu veröffentlichen. So können z.B. die EU-Mitgliedsstaaten LIGHTest nutzen um Listen von qualifizierten *Trust-Services* zu veröffentlichen.

Dieser Beitrag gibt einen Überblick über das LIGHTest-Projekt, die entstandene Referenzarchitektur und mögliche Anwendungsfelder. Der weitere Beitrag gliedert sich wie folgt: In Abschnitt 2 werden verwandte Arbeiten vorgestellt. Abschnitt 3 gibt einen Überblick über die LIGHTest-Referenzarchitektur. In Abschnitt 4 wird eine zentrale Komponente, die *Trust Scheme Publication Authority* (TSPA) genauer betrachtet. Abschnitt 5 stellt die *Trust Policy Language* (TPL) vor, mit der Prüfer von Transaktionen ihre eigenen *Trust Policies* erstellen können. Abschnitt 6 gibt einen Ausblick auf mögliche Anwendungsszenarien bevor in Abschnitt 7 die zentralen Ergebnisse zusammengefasst werden.

Weitergehende Informationen zu einzelnen Teilaspekten von LIGHTest finden sich in weiteren Veröffentlichungen des Projekts ([1],[2],[3],[4],[5],[6],[7]).

Dr. Heiko Roßnagel

ist Leiter des Teams Identitätsmanagement am Fraunhofer-Institut für Arbeitswirtschaft und Organisation.

E-Mail: heiko.rossnagel@iao.fraunhofer.de

Dr. Sven Wagner

ist wissenschaftlicher Mitarbeiter im Team Identitätsmanagement am Fraunhofer-Institut für Arbeitswirtschaft und Organisation.

E-Mail: sven.wagner@iao.fraunhofer.de

2 Verwandte Arbeiten

Die meisten der bestehenden Vertrauensinfrastrukturen basieren auf dem Subsidiaritätsprinzip. Ein prominentes Beispiel ist die eIDAS-Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt [8]. Diese beinhaltet, dass jeder Mitgliedstaat nationale Vertrauenlisten (*Trust Lists*) qualifizierter Ver-

trauensdienstanbieter erstellt und veröffentlicht. Für den Zugriff auf diese vertrauenswürdigen Listen veröffentlicht die Europäische Kommission eine zentrale Liste („*List* of *Trusted Lists*"), die Links zu diesen nationalen Listen enthält.

DANE (*DNS-based Authentication of Names Entities*) ist ein Standard, der DNS und die Sicherheitserweiterung DNSSEC verwendet, um Vertrauen in TLS-Serverzertifikate zu erstellen ([9], [10]). Hierfür wurde der *DNS-Resource Record* TLSA eingeführt, der ein TLS-Serverzertifikat mit dem Domänennamen verknüpft. LIGHTest verfolgt einen ähnlichen Ansatz ist aber nicht auf TLS-Serverzertifikate beschränkt.

Für die Vertrauenslisten gibt es den weit verbreiteten Standard ETSI TS 119 612 [11]. Dieser Standard definiert das Format und die Mechanismen zur Erstellung und Authentifizierung der Vertrauenslisten. Dieser Standard wird auch in LIGHTest verwendet.

3 Referenzarchitektur

Dieser Abschnitt gibt einen Überblick über die LIGHTest-Referenzarchitektur. Hierbei werden das makroskopische Design der LIGHTest-Infrastruktur sowie die Komponenten des Gesamtsystems und deren übergeordnete Funktionalität und Interaktion definiert. Zusätzlich werden in diesem Abschnitt Nutzungsszenarien der Architektur vorgestellt.

3.1 Komponenten der Referenzarchitektur

Abbildung 1 zeigt die LIGHTest-Referenzarchitektur mit allen wichtigen Softwarekomponenten und deren Interaktionen (siehe auch [1], [2]). Es illustriert, wie eine Überprüfung einer empfangenen elektronischen Transaktion basierend auf der individuellen *Trust Policy* des Nutzers und entsprechender Abfragen an die LIGHTest-Vertrauensinfrastruktur durchgeführt werden kann.

Der Nutzer, der eine bestimmte elektronische Transaktion überprüfen möchte, interagiert mit einem Werkzeug zur Erstellung und Visualisierung der *Trust Policies* (z. B. Desktop- oder Webanwendungen). Damit werden auch weniger technikaffine Anwender bei der Visualisierung und Bearbeitung von *Trust Policies*, die für jede Transaktion individuell angepasst werden können, unterstützt. Die *Trust Policy* beinhaltet die formalen Anweisungen für die Validierung der Vertrauenswürdigkeit für die ausgewählte elektronische Transaktion. Zum Beispiel kann definiert sein, welchen *Trust List*s, die auch von mehreren Instanzen ausgestellt werden können, vertraut werden soll. Weitere Details hierzu sind in Abschnitt 5 beschrieben.

Der *Automatic Trust Verifier* (ATV) erhält als Eingangsdaten die elektronische Transaktion sowie die vom Nutzer definierte *Trust Policy* und liefert nach der Prozessierung als Ergebnis, ob die elektronische Transaktion vertrauenswürdig ist oder nicht. Darüber hinaus kann der ATV zusätzlich eine Begründung für seine Entscheidung ausgeben, insbesondere wenn die Transaktion als nicht vertrauenswürdig eingestuft wurde.

Für die *Trust Scheme Publication Authority* (TSPA) wird ein Standard-DNS-Namenserver mit der Erweiterung DNSSEC benötigt. Die TSPA ermöglicht das Finden und Überprüfen der Zugehörigkeit eines Vertrauensdienstes in dem ausgewählten *Trust Scheme*. Dafür ist es erforderlich, dass die Vertrauensdienste in einer oder mehrerer Vertrauenslisten unter den Domänennamen der entsprechenden Instanzen veröffentlicht werden. In Abschnitt 4 wird die TSPA näher beschrieben.

Die *Trust Translation Authority* verwendet ebenfalls ein Standard-DNS-Namenserver mit DNSSEC Erweiterung. Hier werden Listen zur *Trust Translation* veröffentlicht, in denen vertrauenswürdige Behörden anderer *Trust Domain*s aufgelistet sowie mögliche Richtlinien, wie fremde *Trust Schemes* in das eigene *Trust Scheme* übertragen werden können, definiert sind.

Für den *Delegation* Publisher wird der DNS-Namenserver mit DNSSEC Erweiterung zur Ermittlung der IP-Adresse des *Delegation Providers* verwendet. Die Delegationen selbst werden aus Datenschutzgründen nicht im DNS veröffentlicht.

3.2 Anwendungsszenarien

In diesem Abschnitt werden Beispiele für mögliche Anwendungsszenarien kurz vorgestellt. Es gibt sogenannte Basis-Szenarien zur *Trust Publication*, *Trust Translation* und *Trust Delegation* für die qualifizierten Vertrauensdienste qualifizierte Signatur, qualifizierte Siegel, qualifizierte Identifizierung und qualifizierter Zeitstempel. Die Funktionalitäten (*publish, translate, delegate*) der Basis-Szenarien können dann zur Realisierung komplexerer Szenarien weiterverwendet werden. Dies können entweder Varianten der Basis-Szenarien oder eine Kombination verschiedener Basis-Szenarien sein, z.B. eine Verkettung mehrerer Vertrauensdienste. Zum Beispiel *qualified delivery service*, bei denen die Zustellung durch die Kombination der Szenarien für qualifizierte Signatur und qualifizierter Zeitstempel realisiert werden kann. Ein

Abbildung 1 | LIGHTest-Referenzarchitektur (siehe auch [1], [2])

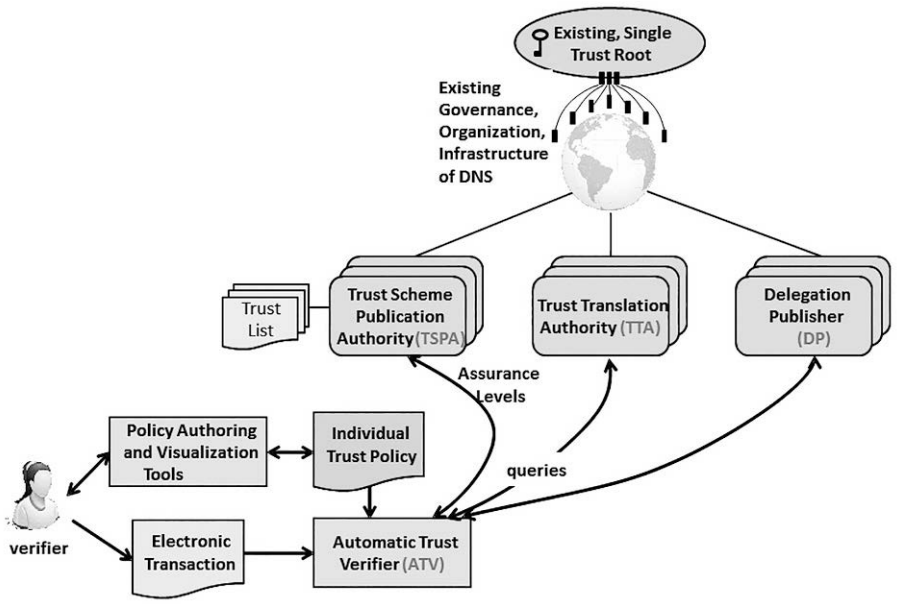
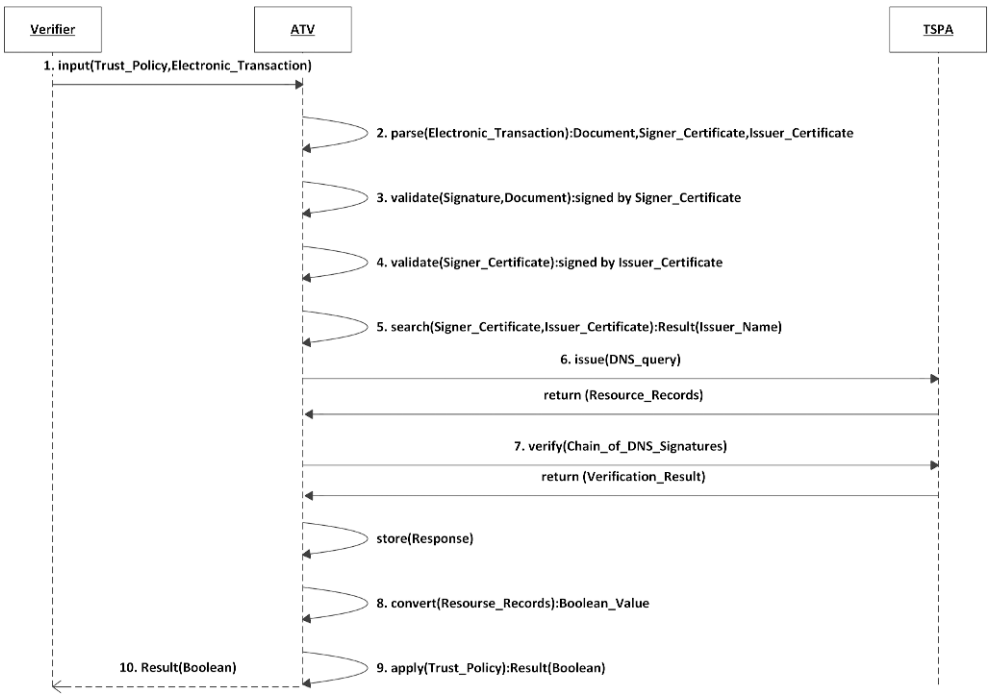


Abbildung 2 | Sequenzdiagramm für Überprüfung einer Trust Scheme Zugehörigkeit [2]



weiteres Beispiel ist die *qualified website authentication*, mit dem Basis-Szenario *Trust Publication* mit qualifizierter Identifizierung und zusätzlich *Trust Translation* zur Authentifizierung von dritten Personen/Dingen.

Als Beispiel für eine erfolgreiche Überprüfung der *Trust Scheme* Zugehörigkeit wird das Basis-Szenario qualifizierte Signaturen im Folgenden kurz dargestellt. Für dieses Beispiel werden die folgenden Voraussetzungen und Annahmen für die elektronische Transaktion und die *Trust Policy* getroffen:

1. Es wird davon ausgegangen, dass sich der Prüfer und Unterzeichner der elektronischen Transaktion in derselben, der EC/eIDAS *Trust Domain* befinden und dass die eIDAS *Trust Domain* das eIDAS *Trust Scheme* enthält. Dies bedeutet, dass in diesem Szenario keine *Trust Translation* erforderlich ist. Dies könnte zum Beispiel in der folgenden Domänennamestruktur verwaltet werden: *Trust.ec.europa.eu – signature – TrustSchemes* – aktuelles eIDAS- *Trust Scheme* für qualifizierte Signaturen.
2. Bei der elektronischen Transaktion wird davon ausgegangen, dass es sich um ein signiertes Dokument handelt. Darüber hinaus enthält das Zertifikat, mit dem das Dokument signiert wird, einen Link zur *Trust List* (*Trust Membership Claim*), z. B. „*Issuer Alt Name: XYZ.qualified.Trust.admin.ec*“. Dieser Link verweist auf die DNS-Einträge des *Trust Schemes* für qualifizierte Signaturen. Darüber hinaus listet dieses *Trust Scheme* das Zertifikat als qualifiziert auf.
3. Für die *Trust Policy* wird angenommen, dass die Signatur des Dokuments als vertrauenswürdig angenommen wird, wenn der Aussteller des Zertifikats in *Trust-Schemes.signature.Trust.ec.europa.eu* aufgeführt ist. Dies entspricht einer booleschen Publikation von *Trust Schemes* (siehe *Abschnitt* 4 für weitere Details).

Für das Basis-Szenario einer erfolgreichen Überprüfung der *Trust Scheme* Zugehörigkeit für qualifizierte Signaturen ist im Folgenden, unter Berücksichtigung der oben genannten Voraussetzungen und Annahmen, der dazugehörige Informationsdatenfluss in der Architektur kurz beschrieben und in Abbildung 2 skizziert.

In Schritt 1 übergibt der Prüfer die elektronische Transaktion und die *Trust Policy* an den ATV. Der ATV extrahiert aus der elektronischen Transaktion das Dokument, das *Signer*- sowie das *Issuer*-Zertifikat (Schritt 2). In Schritt 3 validiert der ATV die Signatur des Dokuments mit Hilfe des *Signer*-Zertifikats. Zusätzlich wird überprüft, ob das *Signer*-Zertifikat vom *Issuer*-Zertifikat signiert ist (Schritt 4). In Schritt 5 durchsucht der ATV das *Signer*- sowie das *Issuer*-Zertifikat nach Informationen zur Zugehörigkeit in einem oder mehreren *Trust Schemes*. In diesem Fall findet der ATV den *Trust Scheme Membership Claim* im *Signer*-Zertifikat „*Issuer Alt Name: XYZ.qualified.Trust.admin.ec*“, und somit wird der *Issuer*-Name aus dem Zertifikat extrahiert. In Schritt 6 kontaktiert der ATV die TSPA, um das zugehörige *Trust Scheme* zu ermitteln. Dafür führt der ATV DNS-Abfragen für alle relevanten Ressourceneinträge für boolesche *Trust Schemes* für „*XYZ.qualified.Trust.admin.ec*“ aus. In Schritt 7 überprüft der ATV die Signaturkette zurück bis zum DNS *Trust Root*. Zusätzlich wird die Antwort dieser Überprüfung für zukünftige, identische Anfragen abgespeichert. Im 8. Schritt wird die Antwort aus den DNS Abfragen in einen booleschen Wert überführt. Im Schritt 9 überprüft der ATV das Ergebnis mit der *Trust Policy* für die elektronische Transaktion und stellt in diesem Fall fest, dass das *Trust Scheme Trust-Schemes.signature.Trust.ec.europa.eu* vertrauenswürdig ist. Daher wird auch nach der Anwendung der *Trust Policy* die elektronische Transaktion als vertrauenswürdig eingestuft, und dieses Ergebnis an den Überprüfer zurückgeschickt (Schritt 10).

Die gezeigte Grundstruktur des Informationsdatenflusses ist auch für die anderen Basisszenarien ähnlich. Bei den qualifizierten Vertrauensdiensten qualifizierte Siegel, qualifizierte Identifizierung und qualifizierter Zeitstempel unterscheidet sich hauptsächlich die Struktur der Domänennamen. Für die Komponenten *Trust Translation* und *Trust Delegation* sind einige zusätzliche Schritte erforderlich, die jeweils mit der dazugehörigen *Trust Translation Authority* bzw. dem *Delegation Publisher* durchgeführt werden.

4 *Trust Scheme Publication* Authority

Die *Trust Scheme Publication Authority* (TSPA) ermöglicht das Auffinden und Überprüfen von Zugehörigkeiten der Vertrauensdienste in einem oder mehreren *Trust Schemes*. Die Veröffentli-

chung von *Trust Schemes* ist immer mit sogenannten *Trust Lists* verbunden, die die Zugehörigkeit des entsprechenden Vertrauensdienstes mit dem referenzierten *Trust Scheme* aufzeigt. Das hier beschriebene Setup für den TSPA ist im Einklang mit aktuellen Standards bezüglich der Verwendung von DNS sowie von *Trust Lists*. Unter anderem wird der existierende und weltweit verwendete Standard ETSI TS 119 612 für *Trust Lists* hier eingesetzt.

Ein *Trust Scheme* kann zum Beispiel die Anforderungen an Informationssicherheitsprozesse, Ausgabe oder Widerruf von *Credentials*, verwendete Technologien oder einfach eine einzige eindimensionale Anforderung, z.B. der geografische Standort, für die zugehörigen Vertrauensdienste festlegen. Werden alle Anforderungen erfüllt, wird der entsprechende Vertrauensdienst als Mitglied des *Trust Schemes* in der dazugehörigen *Trust List* aufgeführt. Dies ist definiert als boolesche Publikation eines *Trust Schemes* [2]. Eine weitere Möglichkeit ist einen ordinalen Aspekt (z. B. verschiedene Sicherheitsniveaus) innerhalb eines *Trust Schemes* zu berücksichtigen. Diese sind definiert als sogenannte *Level of Assurances* (LoAs), und es handelt sich dann um eine ordinale Publikation eines *Trust Schemes*.

Sowohl die Publikation des booleschen als auch des ordinalen *Trust Schemes* beinhaltet keine Informationen über die definierten Anforderungen des entsprechenden *Trust Schemes* bzw. Ordinalwerts (z. B. LoA hoch) des *Trust Schemes*. Für diesen Fall ist eine Tupel-basierte Publikation des *Trust Schemes* erforderlich. Diese beinhaltet die definierten Anforderungen in Form von Tupels mit jeweils einem Attribut und dazugehörigen Wert darzustellen. Die Tupel-basierte Publikation von *Trust Schemes* erfordert hierfür ein einheitliches Datenmodell für alle *Trust Schemes*, bei dem jede Anforderung explizit durch ein Tupel dargestellt ist. Für die Entwicklung dieses Datenmodells wurden neun existierende, nationale und internationale *Trust Schemes* von Behörden (z.B. eIDAS) bzw. aus der Industrie (z.B. FIDO) analysiert und konsolidiert [5]. Das Ergebnis für das einheitliche Datenmodell umfasst die drei abstrakten Konzepte *Credential*, *Identity* und *Attribute* mit insgesamt 98 Konzepten zur Darstellung der definierten Anforderungen. Diese können bei der Tupel-basierte Publikation von *Trust Schemes* an die nach ETSI TS 119612 standardisierte *Trust Lists* als Zusatzinformation hinzugefügt werden.

Das Konzept für die TSPA besteht aus zwei Komponenten: Erstens, ein handelsüblicher DNS-Namenserver mit DNSSEC Erweiterung zur Ermittlung des *Trust Scheme Providers*. Zweitens, der *Trust Scheme Provider*, der die signierten *Trust Lists* zur Verfügung stellt, und darin die Informationen liefert, ob der Vertrauensdienst (z.B. Zertifikatsaussteller) in dem vom *Trust Scheme Provider* betriebenen *Trust Scheme* als vertrauenswürdig eingestuft wird. Die Verwendung von DNS-Namenservern und deren existierenden, globalen Infrastruktur in der LIGHTest-Referenzarchitektur ermöglicht es diesen Ansatz relativ einfach und weltweit für verschiedenste Anwendungsfelder anzupassen und einzusetzen. Die Grundannahme ist jeweils, dass beim Empfang einer signierten elektronischen Transaktion, das dazugehörige *Trust Scheme* des Zertifikatsausstellers für die Signatur noch nicht bekannt ist. Die TSPA bietet hier die Möglichkeit, diese Zugehörigkeit in dem entsprechenden *Trust Scheme* herauszufinden und dieses dann zu überprüfen. Die Ermittlung dieser Zugehörigkeit erfolgt mithilfe der Domänennamenauflösungsfunktionen der DNS-Infrastruktur. Im zweiten Schritt wird der *Trust Scheme Provider* kontaktiert und die Zugehörigkeit des Zertifikatsausstellers in dem entsprechenden *Trust Scheme* überprüft. Für weitere Details zum Konzept der TSPA und zum Vorgehen zur Publikation von *Trust Schemes* sowie zur Abfrage und Überprüfung der Zugehörigkeit von Vertrauensdiensten in *Trust Schemes* verweisen wir auf [2] und [3].

5 *Trust Policy*

Wie bereits in Abschnitt 3 dargestellt, können Nutzer elektronische Transaktionen auf Basis ihrer eigenen, individuellen *Trust Policy* verifizieren. Die dazu benötigten Informationen werden mittels des ATV von den einzelnen beteiligten Instanzen abgefragt. Die individuelle *Trust Policy* beinhaltet formale Anweisungen, welche Voraussetzungen erfüllt sein müssen, damit eine elektronische Transaktion als vertrauenswürdig eingestuft werden kann. Eine *Trust Policy* ist somit eine Art Rezept, das ein oder mehrere *Trust Schemes*, *Trust Translation Schemes* und *Delegation Schemes* als Eingaben verwendet um daraus einen Boolschen Wert über die Vertrauenswürdigkeit der Transaktion als Ausgabe zu generieren. Für die Spezifikation dieses Rezepts wird eine formale *Trust Policy*-Sprache verwendet, die über eine wohl definierte Semantik verfügt und auf mathematischen Formalismen beruht. In LIGHTest wird dafür die Programmiersprache Prolog eingesetzt, die Horn-Klauseln verwendet [6].

Um eine möglichst einfache Erstellung und Visualisierung von *Trust Policies* zu ermöglichen, wurden in LIGHTest mehrere Werkzeuge entwickelt. Diese Werkzeuge erlauben die Erstellung von *Trust Policies* auf drei unterschiedlichen Weisen, welche sich jeweils an spezifische Nutzergruppen richten. So gibt es einen grafischen Editor für Anfänger, mit dem einfache *Policies* erzeugt werden können. Fortgeschrittene Anwender dagegen können einen Editor nutzen, der es ermöglicht vordefinierte Sprachblöcke zu einer *Policy* zusammenzusetzen. Experten können eine Entwicklungsumgebung verwenden um ihre *Policies* direkt in TPL zu programmieren. Im Rahmen von Nutzertests wurden die unterschiedlichen Werkzeuge getestet und evaluiert. Die Ergebnisse zeigen, dass die Nutzer gut mit den vorhandenen Werkzeugen zurechtkamen [7].

6 Anwendungsszenarien

Die LIGHTest-Infrastruktur unterstützt die Umsetzung der eIDAS Regulierung, in dem es die Veröffentlichung bereits existierender *Trust Lists* mit Hilfe von DNS ermöglicht. Darüber hinaus unterstützt LIGHTest den Einsatz von eIDAS auch außerhalb Europas durch die Verwendung eines globalen Vertrauensankers und der Möglichkeit *Translation Schemes* zu erstellen.

Um die Funktionalität der LIGHTest-Infrastruktur zu demonstrieren, werden zwei Pilot-Anwendungen im Rahmen des Projekts implementiert. Im ersten Fall werden LIGHTest-Komponenten in die bereits existierende Cloud-Plattform eCorreos integriert. Hier wird gezeigt, wie LIGHTest die Kommunikation zwischen Unternehmen bzw. Personen und staatlichen Behörden mit den Serviceangeboten der eCorreos Plattform (z.B. MyMailBox) unterstützen, verbessern und vereinfachen kann. In der zweiten Pilotanwendung wird LIGHTest als Komponente innerhalb der OpenPePPOL-Plattform eingesetzt. Hier werden LIGHTest-Komponenten eingesetzt um den von Zeit zu Zeit not-

wendigen Schlüsseltausch beim Wechseln der *Root*-Zertifikate zu unterstützen und zu verbessern, indem für eine definierte Zeitspanne *Trust List*s für die alten und neuen *Root*-Zertifikate existieren. Des Weiteren wird LIGHTest im OpenPePPOL-Pilot zur Authentifizierung von Endnutzern außerhalb der Peppol *Trust Domain* eingesetzt.

Darüber hinaus gibt es zahlreiche weitere mögliche Anwendungsszenarien, die die LIGHTest-Infrastruktur nutzen. Beispielsweise wurde in [12] beschrieben, wie LIGHTest für die Validierung und Authentisierung von Sensordaten in *Predictive Maintenance*-Szenarien im Kontext von Industrie 4.0 eingesetzt werden kann. In [13] und [14] wird ein möglicher Einsatz von LIGHTest beim *Smart Farming* bzw. *Smart City* aufgezeigt.

Aktuell unterstützt das LIGHTest-Projekt die Flüchtlingsorganisation der Vereinten Nationen (UNHCR) bei der Untersuchung wie bestimmte Dokumentationsprozesse, wie z.B. für das DAFI Proramm, digitalisiert werden können. Dabei ist es von entscheidender Bedeutung die Echtheit, Quelle und Vertrauenswürdigkeit von Dokumenten zu bewerten und dokumentieren zu können. Werden bei dem Digitalisierungsprozess die Anforderungen und Standards für die Prozessierung in einem *Trust Scheme* definiert, kann dies sowohl die Verwendung als auch das Sicherheitsniveau der digitalen Dokumente deutlich verbessern.

7 Zusammenfassung

Aufgrund der weltweit stark zunehmenden Anzahl elektronischer Transaktionen besteht ein großer Bedarf an Unterstützung durch Behörden oder anderer Prüfstellen zur Zertifizierung vertrauenswürdiger elektronischer Identitäten. Im Rahmen des EU-finanzierten LIGHTest-Projekts wird eine globale, auf DNS basierte Vertrauensinfrastruktur aufgebaut, in der unabhängige Instanzen ihre Vertrauensinformationen veröffentlichen können. In diesem Beitrag wird zuerst das Projekt vorgestellt und die LIGHTest-Referenzarchitektur sowie zwei zentrale Komponenten daraus (*Trust Scheme Publication Authority* und *Trust Policy*) beschrieben. Die Referenzarchitektur und das Konzept für die *Trust Scheme Publication Authority* erfüllen die erforderlichen Anforderungen für eine global skalierbare Vertrauensinfrastruktur. Darüber hinaus wird der aktuell verwendete Standard für *Trust List*s (ETSI TS 119 612) verwendet und die Anforderungen zur Verwendung von DNS-Namenservern und deren Infrastruktur erfüllt. Die *Trust Policy* ermöglicht den Nutzern elektronische Transaktionen auf Basis ihrer eigenen individuellen Vorgaben zu verifizieren.

Die vielfältige Anwendbarkeit der LIGHTest-Infrastruktur wird in Piloten für e-Correos und Open-PePPOL demonstriert. Zusätzlich gibt es eine Vielzahl weiterer möglicher Anwendungsfällen, z.B im Bereich Sensorvalidierung im IoT und IIoT, oder für große, internationale Organisationen (z. B. UNHCR).

Literatur

[1] Bruegger, B. P.; Lipp, P.: LIGHTest – A Lightweight Infrastructure for Global Heterogeneous *Trust* Management. In: Hühnlein D. et al (Hg.): Open Identity Summit 2016, Rome: GI-Edition, Lecture Notes in Informatics. S. 15-26.

[2] Wagner, S.; Kurowski, S.; Laufs, U.; Roßnagel, H.: A Mechanism for Discovery and Verification of Trust Scheme Memberships: The Lightest Reference Architecture. In (Fritsch, L.; Roßnagel, H.; Hühnlein, D., eds.): Open Identity Summit 2017. Gesellschaft für Informatik, Bonn, 2017.

[3] Wagner, G.; Wagner, S.; More, S.; Hoffmann, H.: DNS-based Trust Scheme Publication and Discovery. Akzeptiert für Open Identity Summit 2019. Gesellschaft für Informatik, Bonn, 2019.

[4] Wagner, G.; Omolola, O.; More, S.: Harmonizing *Delegation* Data Formats. In (Fritsch, L.; Roßnagel, H.; Hühnlein, D., eds.): Open Identity Summit 2017. Gesellschaft für Informatik, Bonn, 2017.

[5] Wagner, S.; Kurowski, S.; Roßnagel, H.: Unified Data Model for Tuple-Based Trust Scheme Publication. Akzeptiert für Open Identity Summit 2019. Gesellschaft für Informatik, Bonn, 2019.

[6] Mödersheim, S.; Ni, B.: GTPL: A Graphical *Trust Policy* Language. Accepted for Open Identity Summit 2019. Gesellschaft für Informatik, Bonn, 2019.

[7] Weinhardt, S.; St. Pierre, D.: Lessons learned – Conducting a User Experience evaluation of a *Trust Policy* Authoring Tool. Akzeptiert für Open Identity Summit 2019. Gesellschaft für Informatik, Bonn, 2019.

[8] European Parliament, 'Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and *Trust* services for electronic transactions in the internal market and repealing Directive 1999/93/EC', European Parliament, Brussels, Belgium, Regulation 910/2014, 2014.

[9] Hoffman, P.; Schlyter J.: The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 0.17487/RFC6698, 2012, http://www.rfc-editor.org/info/rfc6698.

[10] Gudmundsson, O.: Adding Acronyms to Simplify Conversations about DNS-Based Authentication of Named Entities (DANE)", RFC 7218, DOI 10.17487/RFC7218, 2014, http://www.rfc-editor.org/info/rfc7218.

[11] ETSI: Electronic Signatures and Infrastructures (ESI); *Trust*ed *List*s. Sophia Antipolis Cedex, France, Technical Specification ETSI TS 119 612 V1.1.1, 2013; http://www.etsi.org/deliver/etsi_ts/119600_119699/119612/01.01.01_60/ts_119612v010101p.pdf.

[12] Johnson-Jeyakumar, I.-H.; Wagner, S.; Roßnagel, H.: Implementation of Distributed Light weight *Trust* infrastructure for automatic validation of faults in an IOT sensor network. Akzeptiert für Open Identity Summit 2019. Gesellschaft für Informatik, Bonn, 2019.

[13] Wagner, S.; Horch, A.; Kilian, B., Roßnagel, H.: Leichtgewichtige Infrastruktur zur Schaffung von sicherheit und Vertrauen in einem digitalen Ökosystem für Agrardaten. GIL Jahrestagung, Kiel. Gesellschaft für Informatik, Bonn, 2018.

[14] Omolola, O.; More, S.; Wagner, G.; Alber, L.; Fasllija, E.: Policy-based Access Control for the IoT and Smart Cities. Akzeptiert für Open Identity Summit 2019. Gesellschaft für Informatik, Bonn, 2019.