Automating the evaluation of trustworthiness

Marc Sel[1] [0000−0003−3444−1560] and Chris J. Mitchell[2] [0000−0002−6118−0055]

Information Security Group,
Royal Holloway, University of London
Egham, Surrey, TW20 0EX, United Kingdom
Marc.Sel.2013@live.rhul.ac.uk
me@chrismitchell.net

Abstract. Digital services have a significant impact on the lives of many people and organisations. Trust influences decisions regarding potential service providers, and continues to do so once a service provider has been selected. There is no globally accepted model to describe trust in the context of digital services, nor to evaluate the trustworthiness of entities. We present a formal framework to partially fill this gap. It is based on four building blocks: a data model, rulebooks, trustworthiness evaluation functions and instance data. An implementation of this framework can be used by a potential trustor to evaluate the trustworthiness of a potential trustee.

Keywords: Trust · Trustworthiness · Semantics · Ontology · OWL · SPARQL .

1 Introduction

Trust is important because its presence or absence can have a strong influence on what we choose to do or not do, both as individual and as a group. Trusting decisions are made by all of us, often in the context of electronic service delivery. Also automata are increasingly confronted with such decisions. The one that is trusting is commonly referred to as the trustor, the one that is trusted is referred to as the trustee. The trustee may live up to the trustor's expectation, or may let him down. Betrayal of trust is the responsibility of the trustee, not of the trustor. The negative consequences of betrayal of trust may however impact the trustor.

There is a lack of clarity and of agreement on the basic meaning of the terms trust and trustworthiness. Gambetta [4] provides a broad treatment of trust, where in the last chapter the following reasons to trust trust are given.

- If we do not, we shall never find out.
- Trust is not depleted through use, on the contrary.

High level definitions of trust exist but are hard to apply in practical situations. Castelfranchi and Francone [2] state that *'trust is in fact a deficiency of control that expresses itself as a desire to progress despite the inability to control'*.

The term trust carries an ambiguous meaning, as it is used both as a positive and as a negative characteristic. In natural language, trust is perceived as a positive term, such as trust between husband and wife. However, Gollman [5] argues that trust is bad for security. It is remarkable that the European eIDAS Regulation [3], covering trust services and the provision thereof, does not include a definition of trust or trustworthiness.

In the execution of electronic transactions, there are often controls in place, based on service providers such as Trusted Third Parties (TTPs) who claim they can be trusted. However, the use of TTPs based on a Public Key Infrastructure (PKI) lacks a clear definition of trust. In this case trust is expressed through PKI policies which consist of sets of documents, including Certificate Policies and Practise Statements. Semantics is expressed in natural language and formalisms such as Object Identifiers and XML Schema Definitions, which are poor in expressing meaning. Huang and Nicol [6] state that the major PKI specification documents do not precisely define what trust means in PKIs. Rather there are implicit trust assumptions embedded, some of which may not always be true. Such implicit trust assumptions may cause relying parties to have differing understandings about the meaning of certificates and trust.

We address the aforementioned problem by defining a framework that includes a structured process to define requirements, a data model and trustworthiness evaluation functions that are based on these requirements and transformations that adapt real world data to the data model, allowing the transformed data to be stored in a graph database. The practical feasibility of the framework has been demonstrated by a partial implementation of the data model in the Ontology Web Language (OWL), of the evaluation functions in SPARQL, and of the transformations in XSLT. The resulting data was stored in a GraphDB database. The framework allows the use of the semantic interpretations specified by the data model in the evaluations and their outcomes.

The remainder of this article is structured as follows. Section 2 describes the $\mathcal{TE}$ framework and its components. Section 3 describes a partial implementation of the framework, including the creation of instance data based on real-world information and the performance of trustworthiness evaluations on this data. Section 4 presents related work. Section 5 gives conclusions and ideas for future work. The appendix contains selected results from the execution of a sample evaluation as specified in Section 3.

2 The $\mathcal{TE}$ framework

The objective of the $\mathcal{TE}$ framework is to allow a potential trustor to evaluate the trustworthiness of a potential trustee. This evaluation is based on verifying whether a set of rules is satisfied by particular instance data. The framework contains four classes of components: a data model, rulebooks, trustworthiness evaluation functions, and instance data about the potential trustees and their context.

2.1 Defining trustworthiness

The following working definition of trustworthiness is used in the remainder of the article. Trustworthiness is a characteristic of an entity, where entities include persons, ICT systems, organisations and information artefacts, with the properties given below. An entity can be qualified as being ex-ante or ex-post trustworthy, as follows.

- When an entity is qualified as ex-ante trustworthy a trustor can have reasonable expectations that future interactions and their outcomes will be consistent with what has been communicated or committed by the trustee. This is also called forward-looking trustworthiness.
- When an entity is qualified as ex-post trustworthy a trustor can have reasonable expectations that the outcome of a transaction performed in the past can be relied upon. This is also called backward-looking trustworthiness.

2.2 Requirements

The requirements for the framework were developed on the basis of a literature review and the requirements developed in the Horizon2020 FutureTrust project[1] work packages [11], [12]. Requirements from both sources were combined into the following set of integrated requirements.

- IR1 Semantic definition of trustworthiness: *As a participant in an electronic ecosystem I can understand the meaning of trustworthiness of participants I plan to engage with, so that I can make an informed decision on whom to interact with.*
- IR2 Transparency: *As a participant in an electronic ecosystem where I have access to a function that allows me to evaluate trustworthiness of other participants, I can access all information (including inputs used and operations performed) of this function in a transparent*[2] *way, so that I can understand the factors that contribute to trustworthiness and their mapping on evidence such as qualifications of entities.*
- IR3 Linked and unique identity: *As a participant in an electronic ecosystem where I have access to a function that allows me to evaluate the trustworthiness of other participants, I can rely on this function combining all information about participants available within the ecosystem, so that I can claim the outcome of the trustworthiness evaluation is based on all information known about the evaluated participant.*
- IR4 Competently acting in role *As a participant in an electronic ecosystem I have access to and I can demonstrate that I accept the definitions of roles, the qualifications that are required per role, and how these qualifications are demonstrated by participants, so that I can verify these arguments are suitable to support the reliance I want to take on the outcome of the reasoning.*

[1] http://www.futuretrust.eu

[2] The term 'transparent' is used as defined in the Oxford English Dictionary figurative meaning, as 'frank, open, candid, ingenuous' and 'Easily seen through, recognized, understood, or detected; manifest, evident, obvious, clear.'

- IR5 Governance, security and controls: *As a participant in an electronic ecosystem I can understand the governance, security safeguards and controls that are in place within the ecosystem, so that I can claim the outcome of the trustworthiness evaluation took into consideration that the ecosystem meets good practices regarding these topics.*
- IR6 Policy choices: *As a possible participant in an electronic interaction I can determine the information and the reasoning justifying that a participant is qualified as trustworthy, so that I can verify that information and reasoning are compatible with the way I want to rely on the reasoning's outcome.*
- IR7 Obtaining credible data: *As a participant in an electronic ecosystem I can understand the origin and the type of data that is used in the evaluation of trustworthiness of participants, so that I can claim the outcome of the trustworthiness evaluation is based on credible data.*

2.3 Framework participants

The framework positions participants within an ecosystem, structured in three planes as depicted in Figure 1. They may invoke services provided by participants from any plane. The enabler plane consists of the participants whose role is to enable trustworthiness, and it also contains the rulebooks and the trustworthiness evaluation functions which are available to all participants. The roles in this plane are as follows.

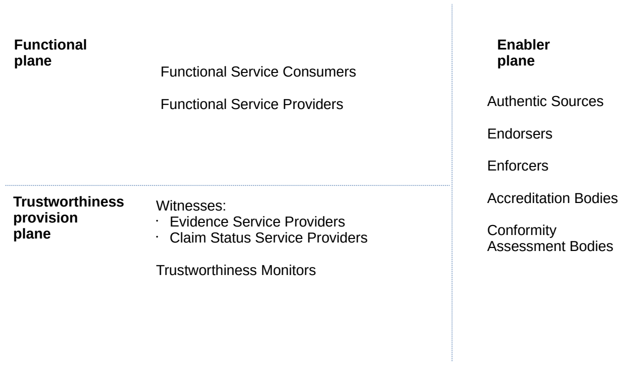
Functional plane
Functional Service Consumers
Functional Service Providers
Trustworthiness provision plane
Witnesses:
· Evidence Service Providers
· Claim Status Service Providers
Trustworthiness Monitors
Enabler plane
Authentic Sources
Endorsers
Enforcers
Accreditation Bodies
Conformity Assessment Bodies

Fig. 1. Planes in a trustworthy ecosystem

- Authentic Source (AS) role. An authentic source holds a mandate to register and validate information about entities and makes this information available. The mandate can be a document that has legal validity because it is published in an official journal or because it is accepted to be binding through a contract or membership agreement.

- Endorser (EnDo) role. An endorser expresses its publicly visible approval for a rulebook through its endorsement, and makes information on responsibility, accountability, and authority to implement security governance available either itself or endorses information made available by others.
- Enforcer (EnFo) role. An enforcer is an entity with power to enforce consequences among participants. An enforcer acts as arbiter or judge and provides the possibility for redress. Enforcement is outside the proposed system[3], but information about whether enforcement is available can be captured and reasoned about.
- Accreditation Body (AB). An accreditation body[4] is an entity that performs accreditation, i.e. the independent evaluation of conformity assessment bodies against recognised criteria for their impartiality and competence. An AB accredits participants in the role of a Conformity Assessment Body.
- Conformity Assessment Body (CAB) role. A CAB assesses the conformity of participants and their services against relevant criteria, and provides assurances of conformity in the form of attestations.

The trustworthiness provision plane involves participants that provide trustworthiness services. The principal roles in this plane are as follows.

- Evidence Service Provider (EvSP) role. An EvSP creates information that serves as evidence. It includes traditional Trust Service Providers such as Certification Authorities, Identity Providers, Attribute Providers, (Remote) Signature Services, Time Stamp Services, etc.
- Claim Status Service Provider (CsSP) role. A CsSP provides status information regarding claims, e.g. verifying a response to an authentication request, or verifying an electronic commitment or signature.
- Trustworthiness Monitor (TwsMo) role. A participant in this role monitors the provision of services by EvSPs and CsSPs and attests to this.

The functional plane consists of participants that act in the role Functional Service Providers (FuSPs), that offer business services, and Functional Service Consumers (FuSCs), that interact with FuSP services.

2.4 Data model

Predicates are used to model the data points that are used for trustworthiness evaluation. The purpose of the predicates is to represent things from the real

[3] One may evaluate the trustworthiness of a credit card provider in a variety of ways, for example that once all other possibilities are exhausted, potential disagreements will be settled before a court of law (an enforcer). Courts of law and all things legal are outside the credit card scheme. Nevertheless I can reason about whether the presence of such an enforcer improves the outcome of evaluation of trustworthiness. Marsh [13] Section 8.5 provides a detailed discussion of the role of an enforcer.

[4] Regarding the roles of Accreditation Body and Conformity Assessment Body, the terminology of ISO/IEC 17000:2020 [7] is adhered to.

world, so that they can be reasoned with. To refer to terms within a predicate, a projection function is used. It can be distinguished from the corresponding predicate by the use of a calligraphic letter in the first position. For example $Predicatename(term_1, term_2)$ is a predicate, and $\mathcal{P}redicatename(term_1, term_2)$ is a projection function. 15 predicates were specified, of which a selection is listed below. S always refers to the Subject.

- $Actor(X)$, an entity without any attestation
- $Attestation(a_{id},\ T)$, where a_{id} = the identity of the issuer of the attestation and triple $T = \{S,\ A,\ V\}$ where A refers to Attribute and V to Value
- $Participant(X)$
- *Base role* specified as $Attestation(a_{id},\ (S,\ roleTypeBase,\ V)$ where V refers to an instance of a role type
- $Accreditation(a_{id},\ (S,\ accreditedFor,\ N)$ where N refers to Norm
- $Conformance(a_{id},\ (S,\ doesConformTo,\ N)$ where N refers to Norm
- $LegalQualification(a_{id},\ (S,\ legalQual,\ L)$ where L refers to a a legal qualification such as a law, regulation, act, or decree

2.5 Rulebooks

The purpose of a rulebook is to formally capture an understanding of what trustworthiness means in a particular context, where this understanding is captured in the form of constraints. A rulebook contains a mandatory and a discretionary part. The mandatory constraints verify the basis for relevant execution of the discretionary rules. The latter can be selected by a potential trustor to configure a policy for trustworthiness evaluation.

Two rulebooks were created inspired by the eIDAS Regulation [3] and according to the specification described in Section 2.2. Rulebook β_{AE} allows the evaluation of the trustworthiness of an ecosystem, and β_{AP} of a participant.

Both rulebooks were constructed as follows. IR1 is addressed by formulating the rules that are derived from the requirements in First Order Logic (FOL) using a taxonomy of data points that have a truth-functional interpretation. While FOL adds value by its truth-functional interpretation, the implementation refines this by using the Organization (ORG) ontology [20] and the Provenance (PROV-O) ontology [19]. This improves interpretation because the ontologies are written in OWL, which allows expression of fine-grained constraints and provides an interpretation in natural language.

Dedicated rules were elaborated, addressing the requirements IR2, IR3, IR4 and IR5 as follows. IR2 is addressed by making the data model, the rules and the trustworthiness evaluation functions publicly available, by using instance data from publicly available sources, and by the specification of IR2 rules. Mandatory rules specify requirements on existence and identification of the rulebook and naming of participants. Discretionary rules specify requirements on the existence of participants in specific roles.

IR3 is addressed by a mandatory rule regarding the uniqueness of identity. Discretionary rules speficy requirements on identity attestation regarding self-attestation, increasingly stringent third-party attestation and legal attestation of identity. IR4 is addressed by a mandatory rule on role attestation regarding self-attestation, and discretionary rules specify increasingly stringent attestation requirements for the different roles, including the legal attestation of roles. IR5 is addressed by discretionary rules that cover disclosure and segregation of duty.

IR6 is addressed by keeping the number of mandatory rules minimal, and allowing the potential trustor to select discretionary rules that correspond best to its policy. IR7 is addressed by selection criteria for data sources from where the instance data will be generated.

A selection of rules is shown in Table 1. S_{pt} corresponds the set of participants and S_{abr} corresponds to the set of role attestations. Projection functions are used, e.g. $\mathcal{A}ttestation_{t_{sub}}(A)$ refers to the subject of attestation A.

Table 1. Sample rules from rulebook β_{AP}

$\beta_{IR4\text{-}M01}$	A participant's base roles must be self-attested	$\forall\ X \in S_{pt}\ \exists\ A_1,\ A_2 \in S_{abr}$ $(\mathcal{A}ttestation_{t_{sub}}(A_1) = f_{id}(X)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{a_{id}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = \mathcal{A}ttestation_{t_{val}}(A_1))$
$\beta_{IR4\text{-}D027A\text{-}AP}$	If the selected participant acts in the role of an evidence service provider then this role must be attested to as conforming to the requirements of an eIDAS TSP by inclusion in a European Trusted List by a trustworthiness monitor	$\exists\ A_1,\ A_2,\ A_3 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}\ (A_1) = f_{id}(P_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}\ (A_1) = R_{EvSP}$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_2) = \mathcal{A}ttestation_{t_{sub}}(A_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = isRegisteredIn$ $\wedge\ \mathcal{A}ttestation_{t_{val}}(A_2) = eIDASTrustList$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}(A_3) = \mathcal{A}ttestation_{a_{id}}(A_2)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}\ (A_3) = R_{TwsMo})$
$\beta_{IR4\text{-}D304\text{-}AP}$	If the selected participant is an evidence service provider or claim status provider, it must be monitored by a trustworthiness monitor attested by a legal act	$\exists\ P_1,\ P_{TwsMo} \in S_{PT}\ \exists\ A_1,\ A_2,\ A_3,\ A_4 \in S_{attn}$ $(\mathcal{A}ttestation_{t_{sub}}\ (A_1) = f_{id}(P_1)$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_1) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}\ (A_1) = (R_{EvSP} \vee R_{CsSP})$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}\ (A_2) = f_{id}(P_{TwsMo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_2) = roleTypeBase$ $\wedge\ \mathcal{A}ttestation_{t_{val}}\ (A_2) = R_{TwsMo}$ $\wedge\ \mathcal{A}ttestation_{a_{id}}(A_3) = f_{id}(P_{TwsMo})$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}\ (A_3) = f_{id}(P_{TwsMo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_3) = doesSupervise$ $\wedge\ \mathcal{A}ttestation_{t_{val}}\ (A_3) = f_{id}(P_1)$ $\wedge\ \mathcal{A}ttestation_{t_{sub}}\ (A_4) = f_{id}(P_{TwsMo})$ $\wedge\ \mathcal{A}ttestation_{t_{att}}(A_4) = legalQual$ $\wedge\ \mathcal{A}ttestation_{t_{val}}\ (A_4) = uri)$

2.6 Trustworthiness evaluation

The trustworthiness evaluation function $twseval_{AE}$ is invoked by a trustor to assist in deciding to what extent an ecosystem represented by instance data can be regarded as trustworthy.

$$twseval_{AE}(R_{id},\ \{DiscretionaryRules\},\ InstanceData)$$

where

- R_{id} identifies the applicable rulebook,
- $\{DiscretionaryRules\}$ denotes the set of discretionary rules selected by the trustor, and
- *InstanceData* identifies the instance data that is to be used.

Execution of the function includes verification of the mandatory rules of the selected rulebook. The function returns *true* when all of the evaluated rules return *true*. *True* means that the evaluated ecosystem meets the constraints specified in the rules, which is an indication of trustworthiness. The function returns *false* when at least one of the evaluated rules returns *false*. *False* means that the evaluated ecosystem does not meet the constraints specified in the rules, which is an indication of a lack of trustworthiness.

The trustworthiness evaluation function $twseval_{AP}$ is used to verify that a participant is trustworthy.

$$twseval_{AP}(RBK_{id},\ P_1,\ target\_base\_role\_X,\ \{DiscretionaryRules\},\ InstanceData,\ \{Norms\})$$

where

- RBK_{id} denotes the identification of the applicable rulebook,
- X denotes the identification of the potential trustee,
- *target_base_role_X* denotes the target base role of X, i.e. the role the trustor would expect the trustee X to act in,
- $\{DiscretionaryRules\}$ stand for the set of discretionary rules selected by the trustor, which allows to configure a trustworthiness evaluation policy, and
- *InstanceData* denotes the reference to the instance data that is to be used,
- $\{Norms\}$ denotes the set of discretionary norms (i.e. legal acts and technical standards) the trustee is expected to provide attestations of conformity assessment to.

The function returns *true* or *false* for each of the evaluated rules.

2.7 Instance data

For the trustworthiness evaluation to be based on credible data, such data must come from authoritative sources that allow access to data that corresponds to one or more predicates. This leads to the following selection criteria. The data source must offer data that is specified in the data model, it must be authoritative for this data, it must include a description of its meaning, and the data must be available in a machine readable format.

There are a number of data sources capable of providing data corresponding to one or more predicates. The current implementation limits itself to data sources in the public domain. On the basis of the selection criteria, the European Trusted Lists[5] and the Linked Open Data source FactForge[6] were selected as data sources for information about companies. On the same basis, a FOAF file from Elsevier's Mendeley Data Search (described by Petrovic and Fujita [16]) and one of the first author's X.509 certificates, produced by the Belgian national identity register, were used as data sources about natural persons.

3 Implementation

The framework was implemented in a front-end and a back-end layer. The front end layer contains the $\mathcal{TE}$ data model, created using Protégé [14], and transformation programs[7] that download information from the data sources and transform it according to the $\mathcal{TE}$ data model, and SPARQL queries whose answers allow to verify the satisfaction of the rules. The back end layer stores the downloaded information as instance data in an Ontotext GraphDB database[8].

The implementation was limited to the evaluation of ex-ante trustworthiness. An evaluation of an entity as a potential trustee involves the following steps. The trustor must connect to the database that holds the instance data, select the discretionary rules of its choice and execute the queries that correspond to the mandatory and selected rules. The query results allow to verify satisfaction of the rules.

Part of an evaluation of an evidence service provider is provided as example. The rules from Table 1 were used, specifying discretionary rules on role attestation. Table 3 shows the results of a query that selects evidence service providers and the provenance of their role attestation. The selection shows a.o. two role attestations for Zetes. The first is based on the Belgian Trusted List and demonstrates satisfaction of IR4-D027A-AP. The second is self-attested and derived from the Zetes website. This demonstrates satisfaction of IR4-M01. Table 4 shows the results of a query that selects participants and their legal attestation. The legal norm can be seen in the right-most column. The selection shows

[5] https://ec.europa.eu/tools/lotl/eu-lotl.xml

[6] http://factforge.net

[7] Developed in a combination of Java and Extensible Stylesheet Language Transformations [21] (XSLTs).

[8] https://graphdb.ontotext.com/

that the legal attestation of Zetes is based on its Certificate Practise Statement, which demonstrates satisfaction of IR4-D304-AP.

The implementation is available online at the following URLs.

- The data model: http://www.marcsel.eu/onto/te/te-data-model.owl.
- A set of instance data: http://www.marcsel.eu/onto/te/DBL.owl.
- The rulebook β_{AE}: http://www.marcsel.eu/onto/te/RuleBook-BAE-FOL.pdf.
- The rulebook β_{AP}: http://www.marcsel.eu/onto/te/RuleBook-BAP-FOL.pdf.
- Trustworthiness evaluation queries that verify satisfaction of the β_{AP} rulebook: http://www.marcsel.eu/onto/te/RuleBook-BAP-SPARQL.txt.

4 Related work

The $\mathcal{TE}$ framework was compared with related work. Its model and reasoning approach are most closely related to Bernabé's SOFIC/Trust-DSS approach [1]. The main similarities are the following.

- Both use the formalisms of an ontology and rules with the aim to support trust-related decisions.
- Both import other ontologies to improve interoperability.

The main differences are the following.

- SOFIC/Trust-DSS approach focuses on decisions related to cloud service providers while the $\mathcal{TE}$ model addresses the broader setting of a potential trustor and a potential trustee.
- The SOFIC/Trust-DSS approach bases its trust-related decision support on an ontology which is security based. The $\mathcal{TE}$ model integrates security data points but does not limit itself to those.
- The SOFIC/Trust-DSS approach involves significant manual effort for the manual translation of observations about a service providers into instances of a SOFIC class, and for the manual customisation of rules in function of what needs to be assessed. The $\mathcal{TE}$ model has automated this translation by the use of XSL, and includes the concept of a rulebook which consists of pre-specified rules.
- The SOFIC/Trust-DSS approach is open to a variety of data sources and rules may be created for specific cases. The $\mathcal{TE}$ model demonstrated its working on actual data imported through the data import and transformation mechanism where the data is formalised in description logic.
- The SOFIC/Trust-DSS approach uses data aggregation and quantification. The $\mathcal{TE}$ model does not, because it is hard if not impossible to define semantics for numbers (what one person rates as 0.7 might be rated otherwise by another person).

A high-level comparison with other related work is given in Table 2.

Table 2. Trust-related ontologies in OWL

Model	**Main objectives**	**Representation formalism**	**Reasoning**
Bernabé [1]	Decision Support System for intercloud trust and security, to allow secure interoperability in a trusted heterogeneous multidomain	Security Ontology For the Inter-Cloud (SOFIC) in OWL	SWRL rules over the ontology and quantification with Fuzzy logic
Karthik [8]	Trust framework for sensor-driven pervasive environments	OWL ontology	Security rules in SWRL
Karuna [9]	Trust model for on-line health information systems	Taxonomy of trust factors and a User's Trust Profile Ontology UTPO in OWL which defines trust factors as classes, taking particularly their relation to the user into account	Recommender algorithms
Kravari [10]	Internet of Things trust management (short paper with only schematic description and implementation)	ORDAIN, general-purpose ontology for trust management, OWL, using RDF/XML	Aggregation and confidence level calculations
Oltramari [15]	Information and decision fusion as a decision support system on trust for humans	ComTrustO, a composite trust-based ontology framework fusion, modelled in OWL, using DOLCE as foundation	Information-based inference and decision fusion
Sel [17]	Trust modelling based on logic	OWL DL and existing vocabularies from W3C	Inference and SPARQL
Sullivan [18]	Definition of security requirements, metrics and trust terms	Ontology for trust-terms defined in OWL, including transparency, measurability, data, accountability, auditing, identification, responsibility, liability	Inference and queries

5 Conclusions and Future Work

The proposed framework demonstrates a possible way to automate the evaluation of trustworthiness. It consists of a data model, rulebooks, a data import and transformation mechanism to create instance data, and queries that verify the satisfaction of selected rules by this data. A potential trustor can select those rules that correspond best to its policy for trustworthiness evaluation. The rules specify requirements regarding the values of a set of data points. Queries allow to verify the satisfaction of these rules. Under the $\mathcal{TE}$ framework, the interpretation of a trust claim is specified as the outcome of the verification of a rule. As a consequence, the meaning of trustworthiness and the interpretations of trust claims are well defined. Furthermore was demonstrated how information from a wide range of data sources can be selected and transformed in the format of the $\mathcal{TE}$ data model, leading to a new way to use existing information to logically reason about trustworthiness.

When compared to the use of trust in TTPs, we argue the proposed $\mathcal{TE}$ model is more precise in terms of semantics regarding the meaning of trustworthiness because it allows a potential trustor to select data points that represent specific information on a potential trustee from a qualified and distributed set of data sources.

The following are candidate topics for future research.

- The potential use of privacy-enhancing techniques to avoid the need for a single linked identity could be investigated.
- The use of legal ontologies could be studied to analyse how additional data points that address legal information could allow expression of legal effects such as presumption of validity and exemption from the burden of proof as components of the evaluation of trustworthiness.
- The possible use of trustworthy hardware and/or software for the creation of attestations could be investigated.
- How independence (or the lack thereof) of participants contributes to trustworthiness could be studied.
- How to create rulebooks for a consensus-governed society rather than for a law-governed society could be investigated. This could include the role of membership organisations such as e.g. the Kantara Initiative[9] as accreditation body and as publisher of a trust list. In such a consensus-governed society the participants must be attested by other participants using a consensus scheme. Many consensus-based schemes that are based on blockchain technology are emerging.
- Regarding the implementation, the use of additional data sources as well as the use of on-line querying rather than the current downloading could be analysed.

Finally, the development of a browser/mail client plug-in that embeds all or parts of the framework is envisaged. This would allow easier experimentation and also access for less technical users.

[9] https://kantarainitiative.org/

References

1. Bernabé, J.B., Pérez, G.M., Skarmeta-Gómez, A.F.: Intercloud trust and security decision support system: an ontology-based approach. J. Grid Comput. **13**(3), 425–456 (2015)
2. Castelfranchi, C., Falcone, R.: Trust and control: A dialectic link. Applied Artificial Intelligence **14**(8), 799–823 (2000)
3. EU: EU 910/2014 Regulation 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, oJ L 257, 28.8.2014, p. 73 114
4. Gambetta, D.: Can we trust trust? In: Gambetta, D. (ed.) Trust: Making and Breaking Cooperative Relations, pp. 213–237. Basil Blackwell, Oxford (1988)
5. Gollmann, D.: Why trust is bad for security. Electronic Notes in Theoretical Computer Science **157**(3), 3 – 9 (2006)
6. Huang, J., M. Nicol, D.: An anatomy of trust in public key infrastructure. International Journal of Critical Infrastructures **13**, 238 (01 2017)
7. ISO/IEC 17000: Conformity Assessment - Vocabulary and general principles. Tech. rep., International Organization for Standardization (2020)
8. Karthik, N., Ananthanarayana, V.S.: An Ontology Based Trust Framework for Sensor-Driven Pervasive Environment. In: AlDabass, D and Shapiai, MI and Ibrahim, Z (ed.) AMS 2017). pp. 147–152 (2017)
9. Karuna, P., Purohit, H., Motti, V.: UTPO: user's trust profile ontology - modeling trust towards online health information sources. CoRR **abs/1901.01276** (2019)
10. Kravari, K., Bassiliades, N.: ORDAIN: an ontology for trust management in the internet of things - (short paper). Lecture Notes in Computer Science, vol. 10574, pp. 216–223. Springer (2017)
11. M. Sel, E. Üstündağ Soykan and E. Fasllija: Deliverable 2.5 on Trust and Trust Models. https://www.futuretrust.eu/deliverables (2017), accessed: 2020-06-20
12. M. Sel, G. Dißauer and T. Zefferer: Deliverable 2.6 Evaluation Scheme for Trustworthy Services. https://www.futuretrust.eu/deliverables (2018), accessed: 2020-06-23
13. Marsh, S.P.: Formalising trust as a computational concept. Ph.D. thesis, University of Stirling (1994), d.Phil. thesis
14. Musen, M.A.: The Protégé project: a look back and a look forward. AI Matters **1**(4), 4–12 (2015)
15. Oltramari, A., Cho, J.: ComTrustO: Composite trust-based ontology framework for information and decision fusion. In: 18th International Conference on Information Fusion, FUSION 2015, Washington, DC, USA, July 6-9, 2015. pp. 542–549 (2015)
16. Petrovic, G., Fujita, H.: Soner: Social network ranker. Neurocomputing **202**, 104–107 (2016)
17. Sel, M.: Improving Interpretations of Trust Claims. In: Trust Management X - 10th IFIP WG 11.11 International Conference, IFIPTM 2016, Darmstadt, Germany, July 18-22, 2016, Proceedings. pp. 164–173 (2016)
18. Sullivan, K., Clarke, J., Mulcahy, B.P.: Trust-terms ontology for defining security requirements and metrics. In: Software Architecture, 4th European Conference, ECSA 2010, Copenhagen. pp. 175–180. ACM (2010)
19. W3C: PROV-O: The PROV Ontology W3C Recommendation 30 April 2013. https://www.w3.org/TR/prov-o/ (2013), accessed: 2020-12-01
20. W3C: The Organization Ontology W3C Recommendation 16 january 2014. https://www.w3.org/TR/vocab-org/ (2014), accessed: 2020-12-01
21. W3C: XSL Transformations (XSLT) Version 3.0 W3C Recommendation 8 June 2017. https://www.w3.org/TR/xslt-30/ (2017), accessed: 2020-12-09

6 Appendix

Table 3. A selection of evidence service providers and the provenance of their role attestation

	EvSP	**Role Attestation**	**wasDerivedFrom**
1	te:Certipost-NV-SA	te:RoleAttestation-Certipost-NV-SA	https://tsl.belgium.be/tsl-be.xml
2	te:Zetes-SA-NV	te:RoleAttestation-Zetes-SA-NV	https://tsl.belgium.be/tsl-be.xml
3	te:Certipost-NV-SA	te:RoleAttestation-Certipost-NV-SA-self	https://www.basware.com/en-en/about-basware/legacy-of-innovation/
4	te:Zetes-SA-NV	te:RoleAttestation-Zetes-SA-NV-self	https://www.zetes.com/en
5	te:SMETS1-PKI-Service-from-SML	te:RoleAttestation-SMETS1-PKI-Service-from-SML-self	https://www.securemeters.com/
6	te:Society-for-Worldwide-Interbank-Financial-Telecommunication-SCRL	te:RoleAttestation-Society-for-Worldwide-Interbank-Financial-Telecommunication-SCRL	https://tsl.belgium.be/tsl-be.xml
7	te:DigiCert-Europe-Belgium-BV	te:RoleAttestation-DigiCert-Europe-Belgium-BV	https://tsl.belgium.be/tsl-be.xml
8	te:Portima-scrl-cvba	te:RoleAttestation-Portima-scrl-cvba	https://tsl.belgium.be/tsl-be.xml
11	te:Belgian-Mobile-ID-SA-NV	te:RoleAttestation-Belgian-Mobile-ID-SA-NV	https://tsl.belgium.be/tsl-be.xml
14	te:Kingdom-of-Belgium-Federal-Government	te:RoleAttestation-Kingdom-of-Belgium-Federal-Government	https://tsl.belgium.be/tsl-be.xml
15	te:Banco-Santander-SA	te:RoleAttestation-Banco-Santander-SA	https://sede.minetur.gob.es/Prestadores/TSL/TSL.xml

Table 4. A selection of participants legally attested in their role

	P1	**Role Attestation of P1**	**LegalRole Qualification**	**LegalNorm**
1	te:BE-BELAC	te:RoleAttestation-AB-BE-BELAC	te:BE-LegalQualification-001	te:BE-Royal-Decree-BELAC-D2014-02-07
2	te:Certipost-NV-SA	te:RoleAttestation-Certipost-NV-SA	te:BE-LegalQualification-003	te:BE-Certipost-CitizenCA-CPS-Version-1.4
3	te:FR-COFRAC	te:RoleAttestation-AB-FR-COFRAC	te:FR-LegalQualification-001	https://www.legifrance.gouv.fr/loda/id/JORFTEXT000019992087/
4	te:FPS-Economy-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:RoleAttestation-TwsMo-FPS-Economy-SMEs-Self-employed-and-Energy-Quality-and-Safety	te:BE-LegalQualification-004	te:BE-LAW-FPS-ECO-BE-SIGN-establishment-2016
5	te:UK-UKAS	te:RoleAttestation-AB-UK-UKAS	te:UK-LegalQualification-001	https://www.legislation.gov.uk/uksi/2009/3155/pdfs/uksi_20093155_en.pdf
6	te:Zetes-SA-NV	te:RoleAttestation-Zetes-SA-NV	te:BE-LegalQualification-007	te:BE-Zetes-CitizenCA-ForeignerCA-CP-CPS-Version-1.1