Empirical Analysis of Trustworthiness Attributes in the Context of Digitization

Sandro Hartenstein
OvGU Magdeburg / HWR-Berlin
Berlin, Germany
e-mail: sandro.hartenstein@hwr-berlin.de

Steven Schmidt
DB Station&Service AG / OvGU Magdeburg / HWR-Berlin
Berlin, Germany
e-mail: s_schmidts19@stud.hwr-berlin.de

Andreas Schmietendorf
HWR-Berlin
Berlin, Germany
e-mail: andreas.schmietendorf@hwr-berlin.de

Abstract— **This paper describes the concept, implementation and first results of a multidimensional research approach to improve the trustworthiness of digital services. It presents the current perception of the concepts of trust and trustworthiness in technical and sociological systems, and their connection as an identified gap. Well-known environmental analysis is used to define the dimensions. The empirical investigations are designed separately for each dimension, or domains of study. The goal is to subsequently create a holistic and robust concept for trustworthy socio-technical systems.**

Keywords - Trustworthiness; Digitization; Information Systems; Society.

I. Introduction

This paper expands the view on the concept, realization and first results of the idea, which was originally and briefly presented at the *The Fourteenth International Conference on Digital Society* 2020, for the empirical analysis of digital services in the context of digitization [1]. The variety of services offered in the digital world is constantly evolving and rapidly increasing due to the establishment of digital aspects in everyday private and professional life. The use of digital services is highly dependent on trustworthiness [2] [3] [4].

However, the concepts of trust and trustworthiness are understood differently in different academic and industrial disciplines, as are the attributes associated with them.

This idea paper aims to present a possible approach to analyze significant factors of trustworthiness through various empirical studies from different fields. The trustworthiness attributes can vary widely from discipline to discipline. In general, it is assumed that these attributes differ mainly only in their weighting, related to the observed discipline for that they are relevant.

This document is divided into six sections. Section I contains the brief introduction. In Section II, different terms and viewpoints on the topic of trust and trustworthiness are described to explain the motivation for this approach. In Section III, past and current related work is then examined, to demonstrate the variations of the current understanding and related contexts that have been evaluated. Section IV describes what could be done to achieve a generic and general model of trustworthiness attributes and associated weights according to the area under study. The conceptional procedure to accomplish this idea is described in detail, as well as what fields are going to be involved as part of the planned project to enable this work. The fields and their individual empirical approach, thus, are presented briefly to demonstrate the general idea of the approach. Section V presents the early results. The outcomes of the analysis of WebAPIs and the survey for public wifis are visualized and explained in the context of trustworthiness. The Section VI contains a summary of the current status of the project and briefly lists the open work packages.

II. Terms & Viewpoints

An agreed-upon definition of trust in the context of digital services is:
“Trust by definition entails a willingness by the [trustor] to make herself vulnerable to the possibility that another will act to her detriment” [5, p. 28], which is also based on the sociological perspective on trust as an fulfilment of expectations towards a person or a system by taking risks [6] [7] [8] [9].

An acceptable definition of trustworthiness in the context of digital services therefore is formed over time and relative to the perception of certain, system specific attributes. Generally, trustworthiness of systems can be defined as being based on ability, benevolence and integrity of the system [10] which correlates with the development of *predictability* over *dependability* to *faith* over time, regarding expectations towards the *persistence*, *technical competence* and *fiduciary responsibility* of a system as shown in Lee and Moray [7], p. 1245. Related approaches tend to a similar characteristic [11] [12] [13].

Digitization depends on the well-being of users. Entrusting data and work steps to a computer system will be criticized by users. In addition to advantages, there are also disadvantages. Trust is the key to accepting digital services, and therefore the key to increasing productivity through digitalization. This creative paper shows the dimensions of trust. These needs are resolved by the supplier. There are several participants with different interests and understandings of trust and trustworthiness.

In the context of the credibility of digital services, the needs of stakeholders are consumers, providers and third-party trustees. Consumers are trying to use services that are as trustworthy as possible, because the impact of data abuse is becoming more and more obvious. Digital service providers need consumer confidence in their products. They also need reliable supply services. The third independent authority can confirm the credibility of the digital service to the user, as long as it has the confidence of the user and can verify the service. From a service point of view, there are two main factors that play a decisive role in its reputation among consumers. User trust and service credibility are these two factors.

In a research project called OPerational Trustworthiness Enabling Technologies, in short OPTET, the prerequisites for trust in the context of Web-based services were determined. The result is that trust can be personal, transferable, and based on core trust, such as in an organization. The credibility of the service is based on its attributes and the attributes confirmed by third parties. Figure 1 summarizes these correlations and their impact [14] [15] [16].

This research focuses on the social, economic, and technological factors that influence trust in digital services, as an implementation of the proposal we presented at the ICDS conference [1]. Based on the analysis of trust and trustworthiness, the following influencing factors can be determined. Social factors can be distinguished by personal, recommendation, and derived trust. Personal trust is characterized by emotions, such as browser authentication status color (red-dangerous, green-good) or knowledge, such as knowledge about two-factor authentication procedures. Recommended trust is based on trusted third parties. Derivative trust is usually formed by the experience of the organization and its status.

The technical factor is the credibility attribute of the service. These should be objectively measured or confirmed by a third party during the development and operation process. Economic factors are characterized by profit expectations.

The provider aims to provide reliable digital services. He can achieve this by optimizing all factors, but each factor must have a minimum level. For example, a certain service may be technically perfect, that is, completely credible, but the provider's reputation is poor, so the derived trust is low, and the service is not entirely credible. One factor that affects consumers is no risk or low risk. If the risk is lower, the service will be more trusted because the potential loss is controllable. However, many users do not realize the value of user data. Therefore, risk assessment is useful for all stakeholders.

Trust in digital services has been shaped by different impacts. The identified influences are personal trust, referral trust and trust in the institution. These findings are based on McKnight's model of trust [17] and Robbins' trust-risk-act model [18] and is visualized in Figure 1. The trust models are briefly explained in the Section III.

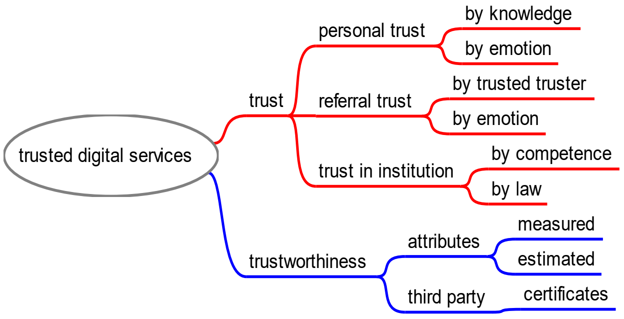


Figure 1. Trust and trustworthiness for digital services [own representation based on [15] [16] [14] [19].

In our view, a holistic view of trustworthiness in the context of digital services that addresses more than quality and security is missing. The possibilities for the technical consideration of services are limited, since only the interfaces are known, not their execution code.

The structure of the well-known Social, Technological, Economic, Environmental, Political, Legal, and Ethical Environment analyses, or STEEPLE, was used to classify the trust-building measures as a view from the outside [20, pp. 80-84]. From the authors' perspective, the environment analysis for a digital service is essential for its trustworthiness and consumer confidence.

In our discussion of trust patterns, we presented the conceptual considerations that trust in WebAPI-based architectures consists of more than just security aspects. We showed that trust develops from personal trust, e.g., in the provider or the technology and trustworthiness of the system. We have classified the trustworthiness attributes ac-cording to product, process and resource in order to determine the appropriate indicators for trust patterns. The categorization is based on the influence on the trust and trustworthiness, which is based on trust aspects [21]. For the OpenAPIs Trustability Parser we also use this classification. The challenge in terms of determining individual values of the attributes, since many indicators are transparent.

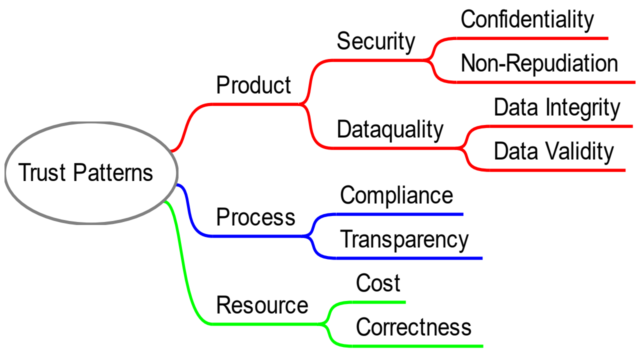


Figure 2. Classification of trustworthiness attributes for trust pattern [21].

III. Related Work

Research on trust has been around for a long time; the basics have been interesting since the 1950s. Recent research has commercial reasons [22]. For trust in software and its use, this section briefly introduces the most important concepts.

The social driver of trust is the honesty, integrity and reliability of the interactive partner. Solving these relationships is the essence of trust. This is also the foundation of social system and market stability. There is no doubt that trust is the basis of everyday interaction.

In early considerations, trust was measured against expected results [23]. If it is good, trust will be established. If the situation is not good, trust will be destroyed. Later, the emotional aspects and the behavior of the participants were identified as important influencing factors [24]. The change in perceptual ability seems to occur mainly in citizens with high trust and little knowledge, and the change in perceived benevolence mainly occurs in citizens with low knowledge and low trust [25].

In a business setting, the cognitive and emotional dimensions of trust were found to be powerful, independent, and interrelated when it comes to building trust relationships with businesses [22]. In a study of the relationship with public institutions, it was found that they are considered more trustworthy than private companies [26]. In a 2001 consideration, all aspects and the implications for trust are integrated into a single design. This is illustrated in Figure 2. Basically, he distinguishes trust in institutions through psychology and sociology that affect personal trust.

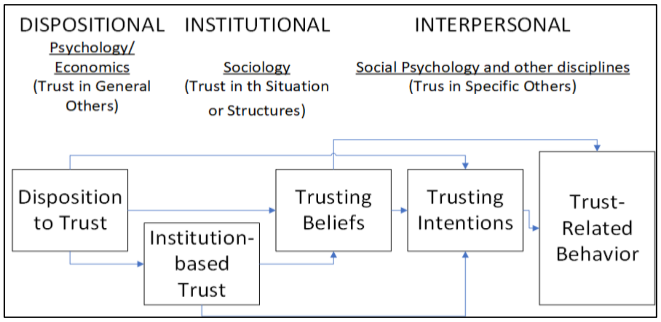


Figure 3. Interdisciplinary model of trust constructs [recreated from 17, p. 33].

An interdisciplinary model of trust was proposed as a modern trust-risk-behavior model, called relational trust [18, p. 985]. It is illustrated in Figure 3 and visualizes the links between trust, risk assessment, and relationships with activities. The factors that affect trust are the characteristics of the actors and the relationship between the actors and external parties.

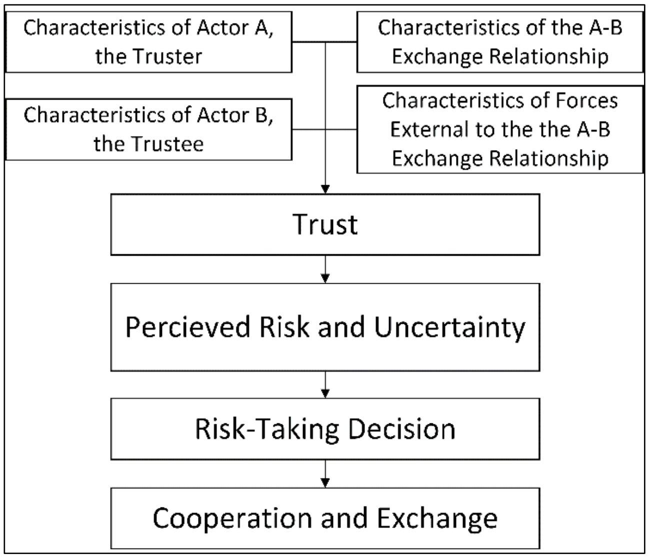

Characteristics of Actor A, the Truster
Characteristics of the A-B Exchange Relationship
Characteristics of Actor B, the Trustee
Characteristics of Forces External to the the A-B Exchange Relationship
Trust
Percieved Risk and Uncertainty
Risk-Taking Decision
Cooperation and Exchange

Figure 4. Structural-cognitive model of trust. [recreated from 18, p. 982].

In the OPTET research project, attributes for trustworthy software were compiled from literature on existing frameworks and surveys in software companies [19, pp. 546-547]. Many attributes were found that represent the nature of a web-based application in terms of its trustworthiness. Since these proper-ties must be evaluated at each point in the life cycle of the application, the main phases with the respective artefacts. A distinction is made between development, marketplace and runtime. In the development phase, the source code is available for analysis. In marketplace phase the software is compiled but not in use. The runtime phase means that the software is operational. Our analysis refers to available WebAPIs, therefore in the runtime context.

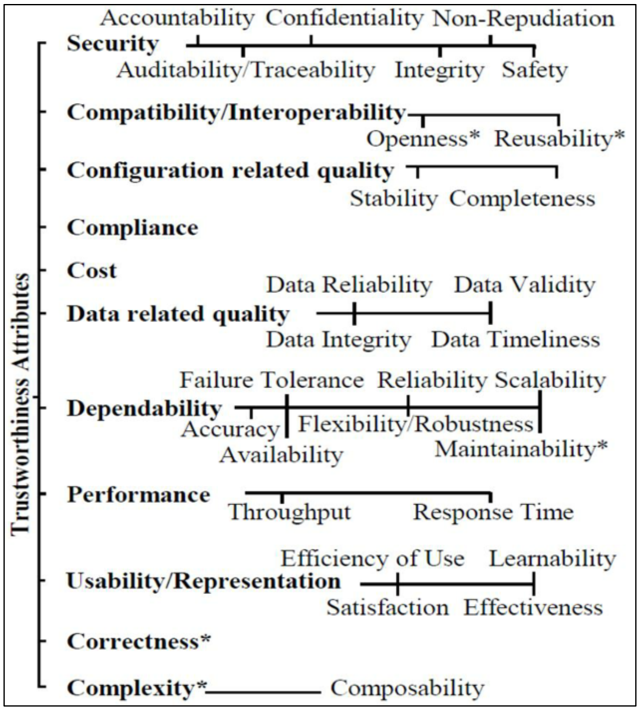


Figure 5. Trustworthiness attributes [27, p. 236].

These attributes have a context-specific impact on credibility. The fields and types of socio-technical systems, referred to as STS, are related. These attributes are measurable and can be influenced by weight mapping.

The top three attributes identified in a study of 72 relevant papers are security, dependability and usability. In almost 2/3 of the literature, security is mentioned as the most important attribute. Almost half of them mentioned reliability. One-quarter of the paper mentions usability as an important attribute of credibility. Figure 5 shows all the attributes and their dependencies [21, p. 25].

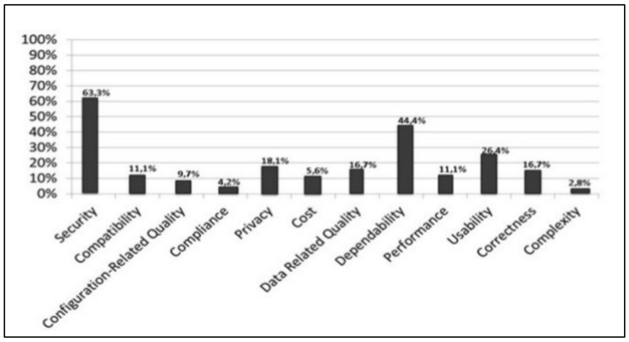


Figure 6. Classified trustworthiness attributes [28, p. 24].

Trustworthiness is an objective property of the WebAPI based primarily on security and quality attributes, but also includes specific attributes such as Complexity, Cost, Privacy, and Compliance [16, p. 14].

Trust is a subjective assessment and differs from the perspective of the respective stakeholder. This assessment is based on knowledge, emotions and expectations of the observer [29, p. 4]. Knowledge in relation to trust states that one understands the rights and duties of a provider and can also understand the measures taken to secure the requirements. Emotion in relation to trust states that one trusts the provider from an inner feeling without knowing the exact measures. The personal risk assessment of a possible misconduct is subjective. Most often, guarantees of the provider are included. The expectations in relation to trust are characterized by the hope that the system will perform the task with trust, because, for example, the function execution is important for the user and he has effort when changing providers [16, p. 11].

APIs, application programming interfaces, are important elements of software development for transparently coupling functionalities, resources and components. Hereby many requirements are fulfilled to the software development. On the one hand can be ensured opposite monolithic systems, an exchangeability and the re-use of particular parts. On the other hand, functions can be outsourced. If this takes place over the public Internet and the functionality as services are offered, we mean WebAPIs. The WebAPIs Economy has several actors. There is the provider, which offers at least one service through a public interface. There is a consumer that integrates these services into its software. This is not limited to one service or one provider. The added value is generated just by combining different services. In between, there can be API brokers that consolidate providers and consumers so that one of the two needs only one point of contact. Furthermore, there is the end user, who uses the consumer's finished application or service [30, p. 19].

The OpenAPI Trustability Parser can support all stakeholders in terms of evaluating the trustworthiness of WebAPIs. For this purpose, it takes the view of the consumer. WebAPIs are implemented for and by software developers and can be used as glue to hold together an increasingly digital world. They shall be specified in a suitable manner so that both the tasks of development-side composition and operationally used communication are supported [30, p. 12].

In our view, a good specification can also provide many indications and statements about individual aspects of trustworthiness. Therefore, the specifications are examined according to the OpenAPI specification [31]. The OpenAPI specification defines a standard for describing Restful APIs. It is promoted by the OpenAPI Initiative, which is supported by the Linux Foundation. Members include Google, IBM, Microsoft and SAP. Operationally, it is implemented by swagger.io, for example [32]. A public directory of WebAPIs according to OAS is provided by APITree.com, for instance [33].

Despite user rates for Wi-Fi access outside people's homes increasing across a range of countries including Germany [34] [35], the limited data published since 2015 indicates user rates only just exceeding 50%, with levels in 2015 at 39% [36] and 55% in 2018 [37] or lower [38]. Usage varies according to provider, with cafes and restaurants (77%) and hotels (88%) at the vanguard [36]. In 2018, user rates shifted slightly in favor of transport infrastructure, with public transport at 60% and mainline railways at 59% [37].

To actually make use of the proposed approach derived from the results of this work for the conception of digital services, the field of Requirements Engineering becomes important. As shown in [39], the field of Service Engineering fits as the wider context, whereas aspects such as Software Engineering or even product Engineering are not to be excluded [40, p. 102]. The general aim is to develop services, that deliver a value to a asking unit as a result or product, by generating a use of potentials and processes of a offering unit whilst market factors are respected [40, p. 58].

The evaluation of the current common systemic view on the matter of the conception of digital services in [39] shows a conceptual lack of possible elicitation, evaluation or management mechanics in current Requirements Engineering approaches within Service Engineering regarding trust building requirements. The underlying definitions of Requirements Engineering for this matter is the knowledge, documentation, specification and management of relevant requirements through process orientation, stakeholder focus and the evaluation of risk and value considerations [41]. This is something that has not yet been applied to the fundamental problem described earlier in [1].

IV. CONCEPT

An environmental perspective becomes important, as different context fields with different environmental factors and thus attuites and requirements a present in this generic approach. The PEST model by [42] originally took four environmental perspectives into account for the analysis: Political, economic, social and technological influences. Younger perspectives extended this approach by ecological, legal and ethical dimensions [20].

In an economical sense this analysis enables market insights as foundation for strategic decisions regarding marketing aspects [43, p. 238]. Regarding the aim of the work described in this paper, it shall serve as an orientation and foundation to cluster requirements coming from or being related to the dimensions.

The concept provides for a multidimensional model of trustworthiness based on the shown STEEPLE environment analysis. The architecture is intended to be designed so that it can be extended by further research in various fields across the sociotechnical spectrum by looking at the STEEPLE dimensions. The initial fields and respective systems considered are as follows:

- **S_1 - Trustworthy WebAPIs.**
  The consideration focuses on the collection and analysis of various trustworthiness-enhancing attributes of WebAPIs. The goal is to investigate the weighting of the different attributes in order to be able to define baseline requirements for digital services.

- **S_2 - Trustworthy public WiFi.**
  The empirical investigation in this area focuses on trustworthiness attributes in public WiFis through questionnaires and comparative interviews between user groups of different services with different trustworthiness levels.

- **S_3 - Trusted AI Web Services.**
  This research area is concerned with identifying and evaluating the trustworthiness of web services that use artificial intelligence in addition to S1, due to more complicated aspects of trustworthiness when it comes to AI approaches.

- **S_4 - Trusted web services of intermediaries.**
  Similar to the previous area, a variety of web presences of self-established mediators will be studied to gain a collection of empirically validated trustworthiness attributes in this area to enrich the proposed overall model with weights unique to this area.

Subarea S_1 deviates from the original idea of simulating the development process [1], since a simulation was assessed as unsuitable upon closer examination. On the one hand, the empery is very limited and on the other hand a theoretical model is already necessary for a simulation. However, this is the goal of the study. Simulation can be used later to evaluate the findings.

Figure 7 shows a schematic representation of the proposed research objective. Each empirically determined trustworthiness attribute (Ai) is to be weighted per system under study (Sj). In addition, these attributes will be categorized according to the STEEPLE dimensions, allowing the formation of clusters. This is helpful to understand system specifications and build a general model. Any further investigation of similar or other systems will add to the overall set, but will also add information about different weights that are unique per area studied. This enables a generic overview over relevant attributes but also a specific derivation for similar systems under consideration in for example Requirements Engineering Frameworks, as this poses a fundamental view of relevant trustworthiness requirements in this field.

In the following two subsections, we present the sub concepts for S_1 and S_2. The S_3 and S_4 sub concepts are currently in the design phase.

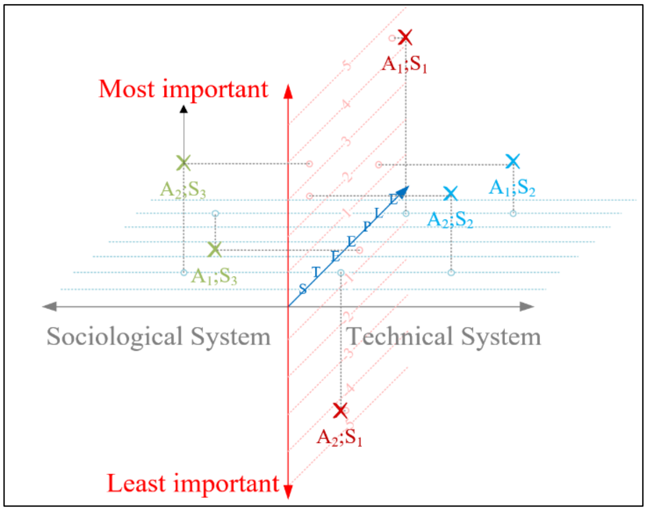


Figure 7. Visualization of the proposed approach.

A. *Concept S_1*

For the first subarea S1 of the project, the empirical investigation of WebAPIs in the context of trustworthiness, the following was designed: The idea is to be able to evaluate the WebAPIs in a structured way according to trust and trustworthiness by parsing OpenAPI specifications. For this purpose, it is necessary to identify indicators for determining the individual attributes and to query them during parsing. Basically, there are two types of indicators that are used for evaluation in relation to trustworthiness attributes. On the one hand, there is the quantitative and on the other hand the qualitative.

The quantitative indicators are countable methods, parameters and data types of the specification. For example, it is relevant how many primary data types and un-structured data types are used. From this, for example, a statement can be made about Data Integrity and its Data Validity. Primary data types are easier to check for integrity in contrast to complex data structures. The attack surface can be deter-mined from the number and type of methods provided. For example, read operations via GET method have much less malicious potential than POST methods. The indicators are used for calculation with the help of metrics in the analysis step. An evaluation can then be made from their results in comparison with defined reference values.

The evaluation of qualitative indicators is significantly more complex, since on the one hand requirements are checked against current requirements and on the other hand several indicators have to be combined. For example, the requirements for authentication and authorization are a good indicator for security, e.g., Confidentiality and Non-Repudiation. The evaluation of the indicator consists of several parts, like the technology, key length and cipher modes. Also, evaluating attributes from the categories of performance, usability and complexity is only possible with qualitative evaluation of the requirements to parameters by the specification. Knowledge of the individual data type is helpful, but not sufficient. Best practices and standards are to serve as reference values for this purpose. Simple metrics are not sufficient at this point, so that further procedures must be used, such as Cosmic function points, as described by us at the IWSM conference [44], or AI analyses.

For these objectives, we have created the following work plan. First of all, it is necessary to find a suitable parser that can capture all indicators and is also integrable. It should also be open and independent of the analysis and evaluation module. In the second step, the parser and a metric analysis should be created with the help of a proto-type. In the third step, the analysis capabilities of the support tool will be exam-ined in a proof of concept with the help of a concrete scenario. In the fourth step, the evaluation of the trustworthiness in the analysis part will be extended.

In the first step, the optimal parser framework was determined. For this purpose, the criteria were defined and evaluated in a decision matrix for each candidate. This is presented in Table 1. The candidates are three Java libraries and two JavaScript modules, where one is deployed as a command line application. The criteria are the supported OpenAPI Standard versions, technical requirements, quantitative and qualitative analysis capabilities. By technical requirements we mean the possibilities to integrate the framework into our tool-chain. Quantitative analysis involves the evaluation of amounts of data types and methods in the specification un-der study. Qualitative analysis includes the capabilities to detect specific methods, such as authentication and authorization, and evaluate them. It also includes the detection of redundant and unnecessary methods and data types. With the help of the respective documentation and test implementations, we have determined that all java candidates fulfill the functional requirements. There are differences in handling and documentation. For this reason, the Swagger parser was selected for the proof of concept. An own developed parser was also considered, but due to the non-specific requirements for trustworthiness in the parsing activity, this was discarded.

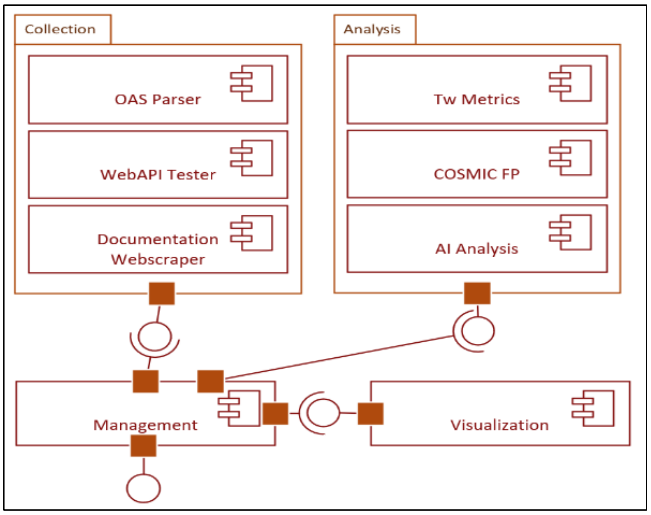


Figure 8. Scheme of software architecture for empirical data collection and processing.

The parser is an important part in the full toolchain for the evaluation of WebAPIs in context of trustworthiness. Additional components are also required for analysis, visualization and management. We chose microservices as our architecture model because it allows us to flexibly integrate different collection and analysis methods. The WebAPIs to be analyzed are captured and tracked via a management component. The architecture concept is shown in Figure 8. The analysis components can also be extended later in this way, so that cosmic function points analysis (COSMIC FP) and machine learning (AI Analysis) can be involved in addition to trustworthiness metrics (Tw Metrics). This architecture also makes it possible to integrate and combine other data collection methods, web scraping and testing.

TABLE 1 DECISION MATRIX FOR PARSING FRAMEWORK

Candidate	Type	OAS	technical requirements	quantitative analysis	qualitative analysis
Swagger-parser [45]	Java library	2 3	can be integrated into Java app; Restful support thereby possible	Simple, all documented methods	Security requirements can be checked if they are present in the Open-Api definition.
Openapi4j [46]	Java library	3	can be integrated into Java app; Restful support thereby possible	Medium, change the specification and subsequent serialization	Security requirements can be checked
KaiZen OpenApi Parser [47]	Java library	3	can be integrated into Java app; Restful support thereby possible	Complex, creates an object, which can be queried. Queries must be created.	Security requirements can be checked if they exist in the object.
Openapi-format [48]	Javascript CLI	3	can be used as a module, thus can be integrated into a NodeJS framework	Complex, prints all methods on the console	Security requirements cannot be checked.
openapi-snippet [49]	Javascript Container	2 3	can be integrated into a JavaScript web framework	Simple, returns an array of the methods	Security requirements cannot be checked.

B. *Concept S_2*

The following was designed for the S2 strand of the project, the empirical investigation of the relevance and perception of trustworthiness in the context of public WiFi as an example of an exposed digital public service.

The idea of the study was to investigate beneficial and restricting factors of public WiFi usage. Existing studies showed a low average usage rate of public WiFis of around 50% of potential users [36] [50] [37]. The evaluation then was supposed to concentrate on the reasons for and against the usage by forming an online questionnaire, which was conducted in Germany. A key element was the representativeness in a demographical way, so results would be accountable for the whole sociological picture. Content wise the survey was divided into different divisions, each focusing on different aspects of public WiFis. After general and statistically relevant questions like age, gender, education etc. data regarding the primarily used mobile device and tendency towards mobile network or public WiFi usage was collected. Following questions concentrated on the aspect of usage factors and personal perception of the relevance and perception of these factors. Part of the questions were explicit, closed answer multiple choice types. Others, to verify or falsify closed questions, were top of mind questions with a free text response option. Collectively they form a representative image on this matter through validation. The last part concentrated on risks and trust concerning public WiFis and the perception of same. Regarding the trustworthiness of such systems, it was also examined, which factors benefit trustworthiness and how they are perceived regarding their importance.

V. Results

In this section, we present the preliminary results of the project areas S_1 and S_2, whose concepts are explained in Section IV.

A. *Results S_1*

In 2018, an investigation of WebAPI specifications was conducted. In this study, the specifications regarding the security requirements were examined. Over 900 WebAPI specifications were examined for security requirements. Only 601 could be automatically parsed and evaluated. The selection of specifications is based on market share in order to be representative. So about 50% are from *Microsoft Azure*, *Amazon AWS* and *Google Cloud*. The survey provides insight into the status of concrete indicators for confidentiality: transport encryption, authentication and authorization. At this point, a repetition of the survey is useful to survey the current state.

As shown in Figure 9, transport encryption is defined at over 90% and over 50% of the specification requires authentication. Over 64% of these expect an OAuth 2.0 token for authentication and authorization [51]. In 2021, the WebAPIs specifications were checked for these same criteria using the new analysis system. Updated specifications were used if they were available. There were 671 specifications valid and could be parsed. The goal is to determine the changes in terms of security and to evaluate the functionality of the prototype. The charts in Figure 9 show the results of the 2018 survey compared to those from 2021. Transport encryption will be supported by almost all WebAPIs in 2021. In the current analysis, 95% of all examined specify HTTPS and only 7% specify the unencrypted HTTP protocol. While in 2018, 17% still specified HTTP. It also requires little effort due to the wide availability of free certificates from *LetsEncrypt*. The benefit in terms of confidentiality outweighs this.

Compared to 2018, the share of WebAPIs that require authentication through their specification has grown from 75% to 82%. WebAPIs without authentication are therefore becoming increasingly rare. In terms of misuse and stability of the APIs, this development is certainly to be welcomed. From a data privacy point of view, this can be assessed differently OAuth 2 is the most frequently offered method for authentication and authorization. Compared to 2018, the share decreased slightly from 64% to 61%. Basic Auth is now only specified for 4% of WebAPIs. Compared with 2018, however, the proportion has fallen slightly from 5% to 4%. The basic authentication of http was also less specified. The percentage of APIs using an API Key has increased from 32% to 39%. The API key is a secret string and often serves as both a unique identifier and a secret token for authentication and authorization.

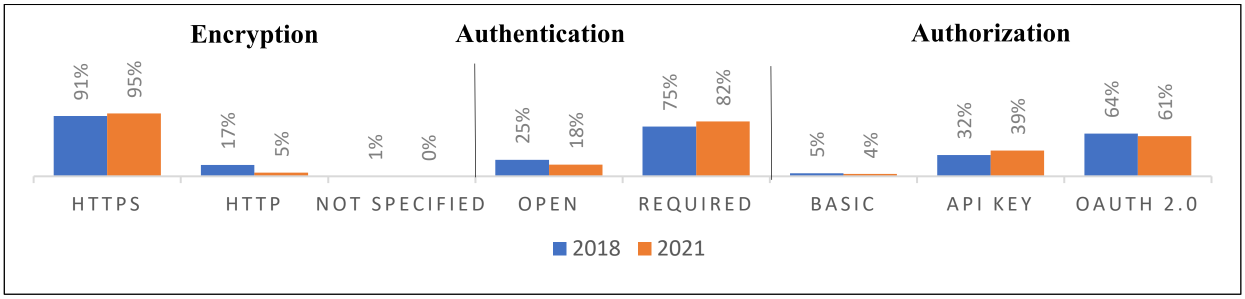
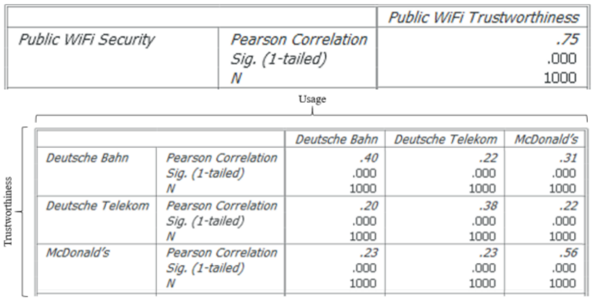


Figure 9. Comparison of the security requirement for WebAPIs from 2018 and 2021 [51].

B. Results S_2

The results have previously been published in [52] and [53] with a deeper statistical analysis of the results. Regarding the specific aim of this paper, the relevant results concern the relevance and perception of trustworthiness attributes and therefore form system requirements for this area. First, it is shown, that the trustworthiness of those systems – like estimated – is rather low at 52.10%. With the security of those systems subjectively evaluated at 40.30% a significant correlation of .75 shows the strong interconnection of security and trustworthiness attributes of a digital service as such, as shown in Figure 10.



		Public WiFi Trustworthiness
Public WiFi Security	Pearson Correlation Sig. (1-tailed) N	.75 .000 1000

Usage

Trustworthiness

		Deutsche Bahn	Deutsche Telekom	McDonald's
Deutsche Bahn	Pearson Correlation Sig. (1-tailed) N	.40 .000 1000	.22 .000 1000	.31 .000 1000
Deutsche Telekom	Pearson Correlation Sig. (1-tailed) N	.20 .000 1000	.38 .000 1000	.22 .000 1000
McDonald's	Pearson Correlation Sig. (1-tailed) N	.23 .000 1000	.23 .000 1000	.56 .000 1000

Figure 10. Evaluations of correlations betweens usage, perceived trustworthiness and security of a system from [53].

This implied the question about the correlation of trustworthiness and usage, whereas the mean of selected service providers formed a correlation of .44 and therefore can be considered as relevant. The underlying implication, that the service provider is a significant factor in this system can be confirmed by the results regarding trust building attributes of a public WiFi, where the service provider was named as the most relevant attribute with 24.35% of all answers, followed by the previously discussed aspects of security at 20.87%, as seen in Figure 11.

Regarding the personal preference of relevant trustworthiness attributes, encryption aspects (66.20%) and a renowned service provider (51.50%) confirm this image as they mark the top two aspects.

As the latter suggests, not only functional requirements were found applicable, as a third-party certification as well as communicative aspects such as the detailed clarification of data usage by the provider where in the lead compared to classical conceptions among public WiFi services such as the acceptance of terms of use etc. Therefore, the presentation of these explicit but nonfunctional requirements has to be taken into consideration, which poses another motivation for the general aim of the presented work.

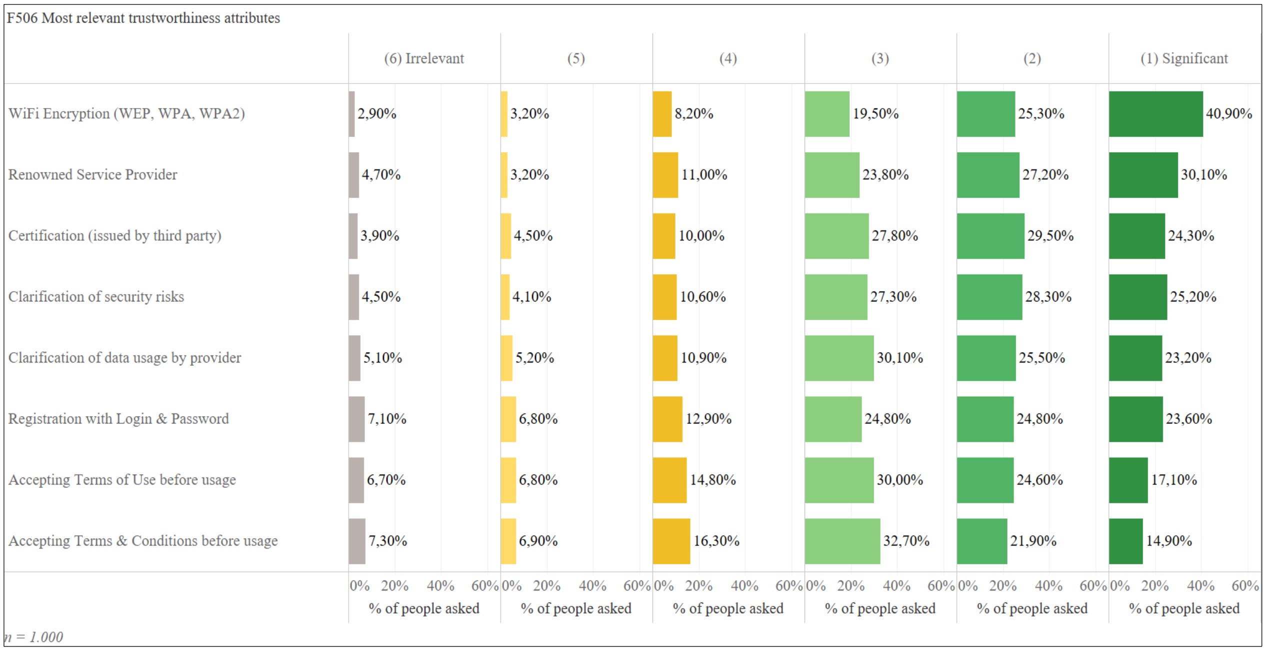


Figure 11. Most relevant trustworthiness attributes of S2 from [53].

VI. Conclusion and Future Work

The initial results of subareas S1 and S2 clearly show that security and quality are important characteristics for trustworthy services. The comprehensible, transparent communication of measures contributes significantly to the acceptance of the services due to a higher trustworthiness. This correlation could also be shown statistically.

In the further progression of the project, we would like to deepen the sub-areas S1 and S2, as well as work on S3 and S4. The S3 subdomain addresses the trustworthiness of AI web services. For this purpose, the trustworthy properties are to be determined with the help of prototypical tests. Part S4 examines the trustworthiness of the mediator profession. With the help of automated web scrapers, findings on this are to be found and linked. A preliminary study conducted in 2019 serves as the starting point for the investigation [54]. The goal is to determine the sociological role in the context of trustworthy web services.

This will allow us to combine the results from the subareas and obtain a multidimensional picture of the trustworthiness of digital services, as described in section IV. The goal is to support the viewpoints with empirical data in order to be able to set up the requirements for trustworthy services in concrete measures.

Continuing this thought process, a framework benefiting from using such a model could be helpful. An assessment on how necessary a generic requirements engineering framework for trustworthy digital services would be can be found in [39], as well as an proposed approach. Basically, a related framework would provide processes, methods and tools as well as provided forms of documentations for requirements engineering. The generic aspect towards including trustworthiness aspects includes a holistic variety of requirements sources for the requirements elicitation, as well as a model to map trustworthiness requirements across functional and non-functional groups, resources, processes and the product in form of a result at the customers end of a digital service. As part of the EUMovE Project and upcoming activities this approach will be further developed and discussed in the future.

References

[1] S. Hartenstein, S. Schmidt, and A. Schmietendorf, “Towards an Empirical Analysis of Trustworthiness Attributes in the Context of Digitalization,” in *The Fourteenth International Conference on Digital Society*, Valencia, Spain, 2020, pp. 112–116. Accessed: Nov. 25 2021. [Online]. Available: https://www.thinkmind.org/articles/icds_2020_3_130_10047.pdf

[2] S. Utz, P. Kerkhof, and J. van den Bos, “Consumers rule: How consumer reviews influence perceived trustworthiness of online stores,” *Electronic Commerce Research and Applications*, vol. 11, no. 1, pp. 49–58, 2012, doi: 10.1016/j.elerap.2011.07.010.

[3] European Commission, *Trustworthy AI.* [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/trustworthy-ai-brochure (accessed: Oct. 16 2020).

[4] World Economic Forum, *Our Shared Digital Future Building an Inclusive, Trustworthy and Sustainable Digital Society: Insight Report.* [Online]. Available: http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf (accessed: Oct. 16 2020).

[5] C. A. Hill and E. A. O'Hara O'Connor, “A Cognitive Theory of Trust,” *SSRN Journal*, 2005, doi: 10.2139/ssrn.869423.

[6] B. M. Muir, *Operators trust in and percentage of time spent using the automatic controllers in a supervisory process control task.* Toronto: University of Toronto, 1989.

[7] J. Lee and N. Moray, “Trust, control strategies and allocation of function in human-machine systems,” *Ergonomics*, vol. 35, no. 10, pp. 1243–1270, 1992, doi: 10.1080/00140139208967392.

[8] M. Söllner and J. M. Leimeister, “What We Really Know About Antecedents of Trust: A Critical Review of the Empirical Information Systems Literature on Trust,” in *Psychology of Emotions, Motivations and Actions, Psychology of trust: New research*, D. Gefen, Ed., Hauppauge, New York: Nova Science Publishers, 2013, pp. 127–155. [Online]. Available: https://www.researchgate.net/publication/262534043_What_We_Really_Know_About_Antecedents_of_Trust_A_Critical_Review_of_the_Empirical_Information_Systems_Literature_on_Trust

[9] C. L. Corritore, B. Kracher, and S. Wiedenbeck, “On-line trust: concepts, evolving themes, a model,” *International Journal of Human-Computer Studies*, vol. 58, no. 6, pp. 737–758, 2003, doi: 10.1016/S1071-5819(03)00041-7.

[10] R. C. Mayer, J. H. Davis, and F. D. Schoorman, “An Integrative Model of Organizational Trust,” *The Academy of Management Review*, vol. 20, no. 3, p. 709, 1995, doi: 10.2307/258792.

[11] Gefen, Karahanna, and Straub, “Trust and TAM in Online Shopping: An Integrated Model,” *MIS Quarterly*, vol. 27, no. 1, p. 51, 2003, doi: 10.2307/30036519.

[12] M. Kohring, *Vertrauen in Medien - Vertrauen in Technologie*. Stuttgart: Akademie für Technikfolgenabschätzung in Baden-Württemberg, 2001. [Online]. Available: http://elib.uni-stuttgart.de/handle/11682/8694

[13] R. Kuhlen, “Vertrauen in elektronischen Räumen,” in *Informationelles Vertrauen für die Informationsgesellschaft*: Springer, Berlin, Heidelberg, 2008, pp. 37–51. Accessed: Nov. 11 2021. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-77670-3_3

[14] S. van der Graaf, W. Vanobberghen, M. Kanakakis, and C. Kalogiros, “Usable Trust: Grasping Trust Dynamics for Online Security as a Service,” vol. 9190, pp. 271–283, 2015, doi: 10.1007/978-3-319-20376-8_25.

[15] A. Chakravarthy *et al.,* “OPTET D2.4 Socio-economic evaluation of trust and trustworthiness,” OPTET. Accessed: Oct. 16 2020. [Online]. Available: https://www.researchgate.net/publication/317488309_OPTET_D24_Socio-economic_evaluation_of_trust_and_trustworthiness

[16] S. Wiegand *et al.,* “D2.5 – Consolidated report on the socio-economic basis for trust and trustworthiness,” OPTET, 2015. Accessed: Oct. 16 2020. [Online]. Available: https://www.researchgate.net/publication/317488377_OPTET_D25_-_Consolidated_report_on_the_socio-economic_basis_for_trust_and_trustworthiness

[17] D. H. McKnight and N. L. Chervany, “Trust and Distrust Definitions: One Bite at a Time,” in *Lecture Notes in Computer Science*, vol. 2246, *Trust in Cyber-societies: Integrating the*

Human and Artificial Perspectives, R. Falcone, M. Singh, and Y.-H. Tan, Eds., Berlin, Heidelberg: Springer, 2001, pp. 27–54.

[18] B. G. Robbins, “What is Trust? A Multidisciplinary Review, Critique, and Synthesis,” *Sociology Compass*, vol. 10, no. 10, pp. 972–986, 2016, doi: 10.1111/soc4.12391.

[19] N. Gol Mohammadi *et al.,* “An Analysis of Software Quality Attributes and Their Contribution to Trustworthiness,” *Proceedings of the 3rd International Conference on Cloud Computing and Services, Science*, pp. 542–552, 2013.

[20] G. Johnson, K. Scholes, and R. Whittington, *Strategic Management [orig.: Strategisches Management]: An Introduction; Analysis, Decision and Implementation [orig.: Eine Einführung; Analyse, Entscheidung und Umsetzung],* 9th ed. München: Pearson Studium, 2011.

[21] S. Hartenstein, S. Schmidt, and A. Schmietendorf, “Trust Patterns in Modern Web-API Based Service Architectures - More than Technical Security Aspects,” in *Patterns 2021*: IARIA, 2021, pp. 23–25. Accessed: May 5 2021. [Online]. Available: http://thinkmind.org/articles/patterns_2021_2_10_70007.pdf

[22] A. Patrick, S. Marsh, and P. Briggs, “Designing Systems That People Will Trust,” *Security and Usability*, NRC 47438, pp. 75–99, 2005. [Online]. Available: https://www.researchgate.net/profile/Pamela_Briggs/publication/44081283_Designing_Systems_That_People_Will_Trust/links/00b7d5344d8b27f675000000.pdf

[23] G. Simmel, *The sociology of Georg Simmel: Selected writings*. New York: Free Pr, 1964.

[24] D. Trček, “A Brief Overview of Trust and Reputation over Various Domains,” in *SpringerBriefs in Information Systems, Trust and Reputation Management Systems: An e-Business Perspective*, D. Trček, Ed., Cham: Springer International Publishing, 2018, pp. 5–19.

[25] T. Nguyen, “Trust and Sincerity in Art,” *Ergo*, 2020. [Online]. Available: https://www.researchgate.net/publication/343239976_Trust_and_Sincerity_in_Art

[26] S. G. Grimmelikhuijsen and A. J. Meijer, “Effects of Transparency on the Perceived Trustworthiness of a Government Organization: Evidence from an Online Experiment,” *JOPART*, vol. 24, no. 1, pp. 137–157, 2014, doi: 10.1093/jopart/mus048.

[27] S. Paulus, N. G. Mohammadi, and T. Weyer, “Trustworthy Software Development,” in *Lecture Notes in Computer Science, Communications and Multimedia Security*, D. Hutchison et al., Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 233–247.

[28] N. G. Mohammadi *et al.,* “Trustworthiness Attributes and Metrics for Engineering Trusted Internet-Based Software Systems,” in *Communications in Computer and Information Science, Cloud Computing and Services Science*, M. Helfert, F. Desprez, D. Ferguson, and F. Leymann, Eds., Cham: Springer International Publishing, 2014, pp. 19–35.

[29] A. Hoffmann, H. Hoffmann, and M. Söllner, “Twenty Software Requirement Patterns to Specify Recommender Systems that Users Will Trust,” *ECIS 2012 Proceedings.Paper 1*, 2012. [Online]. Available: https://www.alexandria.unisg.ch/228939/1/Hoffmann%20et%20al.%202012.pdf

[30] S. Hartenstein, K. Nadobny, S. Schmidt, and A. Schmietendorf, *Sicherheits- und Compliance-Management im Lebenszyklus von Web APIs: Ergebnisse eines Forschungsprojektes an der HWR Berlin/Uni Magdeburg*. Berlin: Logos-Verlag, 2020.

[31] OpenAPI Initiative, *OpenAPI Specification.* [Online]. Available: https://spec.openapis.org/oas/v3.1.0 (accessed: May 3 2021).

[32] SmartBear Software, *Swagger.* [Online]. Available: https://swagger.io/ (accessed: May 21 2021).

[33] ApiTree, *APITree Hub.* [Online]. Available: https://www.apitree.com/ (accessed: May 21 2021).

[34] iab Austria, *ondevice research.* [Online]. Available: http://www.iab-austria.at/wp-content/uploads/2015/07/IAB-Mobile-Video-Usage-FINAL.pdf

[35] Eurostat, *Eurostat - Data Explorer,.* [Online]. Available: http://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do

[36] A. Grieß, *Nur Minderheit nutzt WLAN außerhalb der eigenen vier Wände.* [Online]. Available: https://de.statista.com/infografik/3575/nutzung-von-fremden-wlan-netzen/ (accessed: Mar. 6 2021).

[37] EarsandEyes GmbH, *Öffentliches WLAN in Deutschland.* [Online]. Available: https://www.earsandeyes.com/download/wlan-report

[38] Statista, *Beliebteste Nutzungsorte von WLAN 2018 | Statista.* [Online]. Available: https://de.statista.com/prognosen/953712/umfrage-in-deutschland-zu-den-beliebtesten-nutzungsorten-von-wlan (accessed: Feb. 20 2021).

[39] S. Schmidt, “Zur Notwendigkeit eines generischen Requirements Engineering Frameworks für vertrauenswürdige IT-Services,” in *Berliner Schriften zu modernen Integrationsarchitekturen*, vol. 25, *Online-Workshop (e) trust – Vertrauen in Digitale Dienste (Werte – Risiken – Prinzipien – Methoden – Techniken)*, A. Schmietendorf, Ed., 1st ed., Düren: Shaker Verlag, 2021.

[40] H.-J. Bullinger and A.-W. Scheer, Eds., *Service Engineering: Entwicklung und Gestaltung innovativer Dienstleistungen ; mit 24 Tabellen,* 2nd ed. Berlin: Springer, 2006.

[41] M. Glinz, *A Glossary of Requirements Engineering Terminology.* Accessed: Jul. 21 2021. [Online]. Available: https://www.merlin.uzh.ch/contributionDocument/download/9869

[42] C. Bowman, *Strategy in practice*. Harlow: Prentice Hall Financial Times, 1998.

[43] H. Meffert, C. Burmann, and M. Kirchgeorg, *Marketing: Grundlagen marktorientierter Unternehmensführung ; Konzepte, Instrumente, Praxisbeispiele,* 10th ed. Wiesbaden: Gabler, 2008.

[44] S. Hartenstein, K. Nadobny, S. Schmidt, and A. Schmietendorf, “An Approach for a Fast Cost Validation of Web-Based APIs supported by Functional Size Measurement with COSMIC,” in vol. 2476, *IWSM-Mensura 2019: International Workshop on Software Measurement and International Conference on Software Process and Product Measurement 2019*, Ayca Kolukisa Tarhan, Ahmet Coskuncay, Ed., Haarlem, The Netherlands: CEUR Workshop Proceedings, 2019, pp. 103–111. Accessed: Oct. 21 2019. [Online]. Available: http://ceur-ws.org/Vol-2476/short2.pdf

[45] *swagger-parser.* [Online]. Available: https://github.com/swagger-api/swagger-parser (accessed: May 12 2021).

[46] *openapi4j.* [Online]. Available: https://github.com/openapi4j/openapi4j (accessed: May 12 2021).

[47] *KaiZen-OpenApi-Parser.* [Online]. Available: https://github.com/RepreZen/KaiZen-OpenApi-Parser (accessed: May 12 2021).

[48] *openapi-format.* [Online]. Available: https://github.com/thim81/openapi-format (accessed: May 12 2021).

[49] *openapi-snippet.* [Online]. Available: https://github.com/ErikWittern/openapi-snippet (accessed: May 12 2021).

[50] EarsandEyes GmbH, *Report Öffentliches WLAN in Deutschland (Public WLAN in Germany Report).* [Online]. Available: https://www.earsandeyes.com/wp-content/uploads/2019/05/EARSandEYES_Report_%C3%96ffentliches_WLAN.pdf (accessed: Feb. 2 2020).

[51] A. Reichenbach and A. Schmietendorf, "Empirische Untersuchung zur Open API Spezifikationen," in *Berliner Schriften zu modernen Integrationsarchitekturen*, Band 18, *API-First/API-Management - Open APIs als Treiber der Digitalisierung: Workshop im Rahmen der Enterprise Computing Conference, 19. April 2018, Hamburg*, A. Schmietendorf and A. Nitze, Eds., 1st ed., Aachen: Shaker, 2018, pp. 1–28.

[52] S. Schmidt, "Schaffung eines vertrauenswürdigen, öffentlichen WLANs - Herangehensweise und Teilergebnisse," in *Berliner Schriften zu modernen Integrationsarchitekturen*, vol. 24, *ESAPI 2020: 4. Workshop Evaluation of Service-APIs*, A. Schmietendorf and K. Nadobny, Eds., 1st ed., Düren: Shaker, 2020, pp. 35–48. Accessed: Jul. 17 2021. [Online]. Available: https://www.researchgate.net/publication/345081598_Schaffung_eines_vertrauenswurdigen_offentlichen_WLANs_-_Herangehensweise_und_Teilergebnisse

[53] S. Schmidt, "On the perception and relevance of trustworthiness in public wireless networks," in *Advances in Security, Networks, and Internet of Things: Proceedings from SAM'21, ICWN'21, ICOMP'21, and ESCS'21*, 2021.

[54] W. H. Letzel and A. Schmietendorf, "Digitalisierung und Mediation aus der Anwenderperspektive," no. 1, 4-10, 2019.