# Certification Matters for Service Markets

Marie-Christine Jakobs, Julia Krämer, Dirk van Straaten and Theodor Lettmann

Paderborn University
Paderborn, Germany
Email: {marie.christine.jakobs,juliadk,dirk.van.straaten,lettmann}@upb.de

***Abstract*—Whenever customers have to decide between different instances of the same product, they are interested in buying the best product. In contrast, companies are interested in reducing the construction effort (and usually as a consequence thereof, the quality) to gain profit. The described setting is widely known as opposed preferences in quality of the product and also applies to the context of service-oriented computing. In general, service-oriented computing emphasizes the construction of large software systems out of existing services, where services are small and self-contained pieces of software that adhere to a specified interface. Several implementations of the same interface are considered as several instances of the same service. Thereby, customers are interested in buying the best service implementation for their service composition wrt. to metrics, such as costs, energy, memory consumption, or execution time. One way to ensure the service quality is to employ *certificates*, which can come in different kinds: *Technical* certificates proving correctness can be automatically constructed by the service provider and again be automatically checked by the user. *Digital* certificates allow proof of the integrity of a product. Other certificates might be rolled out if service providers follow a good software construction principle, which is checked in annual audits. Whereas all of these certificates are handled differently in service markets, what they have in common is that they influence the buying decisions of customers. In this paper, we review state-of-the-art developments in certification with respect to service-oriented computing. We not only discuss how certificates are constructed and handled in service oriented computing but also review the effects of certificates on the market from an economic perspective.**

***Keywords–Service; Certification; Service-Oriented Computing.***

## I. Introduction

In today's complex world, it is nearly impossible to base decisions on sufficient knowledge about all relevant facts. One way around this dilemma is to make use of certification. According to Wikipedia [1], *certification refers to the confirmation of certain characteristics of an object, person, or organization.* Real-life examples are manifold, from professional certifications, such as master's degrees awarded by universities, to product certification such as the CE conformity marking in the European Economic Area. Especially, professional certification often denotes not only procedures for validating expertise before granting a certificate, but also programs by which necessary competences are developed. Here, we restrict ourselves to the impact of the final certificates on a market. Certificates provide a certain amount of evidence that some required characteristics of a good, a person, or a process are given. No further testing is needed, except for testing the validity of the certification itself. Therefore, using widely adopted certifications is a key issue for increasing the competitiveness of a company. However, if a third party, usually a government agency, is interested in establishing minimum standards, we talk about licensing and accreditation instead of certification. Whereas, licensing is a non-voluntary process used as an entry condition of a market, accreditation is a voluntary process granting (public) recognition, e.g., for schools or universities. In this paper, we want to take a closer look at the role of certification in a service-oriented computing market.

*Service-oriented computing* aims at facilitating the construction of large software systems by assembling existing services. We consider services as a single, platform-independent piece of software that is specified using an interface. Service-oriented computing gives rise to a global market where numerous service providers offer their own implementations of specific services and where services of different providers interoperate with each other in *service compositions* to deliver highly customized software to users. In service compositions, a single faulty or data-leaking service may ruin the overall correctness or privacy requirements. This is a crucial characteristic of service-oriented computing as it might lead to unsatisfied customers resulting in a drop of market efficiency and finally in a market failure [2]. This can be prevented by installing quality-ensuring mechanisms that provide quality signals to customers and, hence, enable them to choose the best fitting service provider.

In online shops, it is common practice to use the reputation provided by customer reviews [3] as a quality signal. In this case, previous customers rate the delivered product or service according to their own experience. Although this quite simple example of a reputation system works well in many domains, there are some drawbacks in markets for highly specialized goods such as markets for service-oriented computing. First, since service quality is reported by users, there must be a reasonable number of people willing to provide ratings for the same service, otherwise no measure of quality exists. Because of the diversity of services and service compositions and their continuous improvement, many users will have to run services without any prior information about service quality. Second, customer ratings are subjective by nature and therefore not an objective quality signal. As service quality and performance depends on the use case, there is an additional source of unreliability. Since services are not only offered by a few well-known global players but also by unknown and untrusted entities, a reliable source for service quality information is necessary, in particular in markets for service-oriented computing.

*Certification* is not yet another mechanism to signal the quality of services even for inexperienced end-users. In contrast to reputation, certificates can allow judging the quality of a service or a service composition directly when it is available in the market and, thus, especially before any user might be annoyed or even harmed by a bad-quality service. In addition, the producer of a service himself is responsible for this type of trust management and bears the risk of abuse. Hence, certificates are a customer-friendly, complementary instrument besides reputation when it comes to signaling service quality. Theoretical results support this complementary interaction for certain market models [4].

*Contribution.* In this paper, we study certificates in service markets as a complementary approach to signal quality. On the basis of the app store example, we define all ingredients of certification in service markets that may influence the validity of a certificate. We also review state-of-the-art literature in certification wrt. to service-oriented architectures and introduce a taxonomy to classify existing approaches. Additionally, we discuss the need for certification in service markets and identify open challenges for certification in these markets.

This paper is organized as follows. In Section II, we give an overview of certification, introducing the ingredients of certification, and reviewing existing certification approaches. Section III introduces our taxonomy for certificates and classifies the reviewed certification approaches. Section IV highlights the need for certification in service markets from an economic perspective before the corresponding challenges are discussed in Section V. Finally, Section VI concludes the paper.

## II. Overview of Certification

Markets in which software products are assembled and delivered on-the-fly give rise to intricacies in quality assurance. We think that these intricacies in quality assurance cannot be solved by *solely* using reputation systems and that they challenge the application of standard certification techniques. In this section, we use *app stores* as an instance of on-the-fly service markets to introduce important ingredients of certification.

*App Stores as On-The-Fly Service Markets:* Nowadays, smartphones often run many different apps at the same time. Often, these apps interoperate with each other. While it simplifies daily life if tasks, calendars, mails etc. are automatically kept consistent across platforms and apps, it carries a tremendous risk for the safety and privacy of user data. Typically, cross-platform consistency is achieved by storing the data in cloud storage. If such a service for cloud storage goes out of business, important data such as notes, mails and contacts might be lost forever. If these cloud services sell private user data, companies using these services might go out of business themselves. To complicate things, different service providers offer different apps realizing the same functionality – some of them might be free of charge, available only for a certain type of Android device, or might consume more or less space. Hence, users not only need to know *which* functionality they want to buy, but also need to have the chance to make informed decisions in favor or against certain providers or apps in order to find the most *reliable* provider and the app with the highest *quality* among all the existing options.

Instead of estimating the quality of a software and the reliability of a provider on the basis of user recommendations or previous experiences with other products of the same provider, nowadays, customers use certificates indicating quality such as expert recommendations or editors' choices of good apps, award winning apps, top or featured developers, apps with signed Android application packages (APKs), or trusted apps. In the following, we restrict ourselves to these examples to explain the ingredients of certification.

### A. Ingredients of Certification

Essentially, *certification* is the process of attesting a specified (minimum) qualification, quality, or standard by granting a *certificate* [1] [5]. Standards to meet and guidelines for the certification process are often developed by organizations of interested parties. The certification process itself is performed by an (accredited) *certification body*. In the app store example, the roles of the standard-defining organization and the certification body issuing the certificate often coincide due to rapid advancements and missing established standards in this field. In the recommendation example, the certification body is the expert writing the recommendation, whereas the developer himself signs apps with APK keys and is thus the *certification body* in the APK key example.

The *scope of certification* identifies the entity (e.g., product, process, service) that the certification is granted for, the standard or normative document stating the *certification criteria*, and the *certification scheme* that specifies rules and procedures for testing conformity with the standard. The certifications mentioned in the app store example vary widely wrt. their scope. For instance, recommendations and signed APK keys certify single apps, whereas listings of featured developers certify app providers. As a result of a certification, a *certificate* is granted which is an accreditation that the scope of certification is met, i.e., the entity conforms to the standards wrt. the certification criteria tested. This implies that certification criteria should be objective and comparable requirements. The examples show that certificates have different *certification credibility*. Signed APK keys are digital proofs of the identity of the developer and, thereby, an objective criterion, whereas experts, which have personal preferences, may write recommendations rather subjectively. The *certificate checker* [6] [7] is the entity validating a certificate. In most cases, this will be the user. Referring to the term *trusted computing base*, we use the term *trusted base* to denote all ingredients of the certification process, which one needs to rely on to trust the certification technique. We continue with an overview of existing certification approaches (including our examples from this section) in the context of service markets.

### B. Overview of Existing Certification Approaches

A broad range of certification techniques can be found in the literature and in practical use. To simplify the following discussion, we separate the presentation of the existing approaches of certificates along technical and documentary evidence. Technical evidence carries machine processable information to reinvestigate if the certification criteria are met while documentary evidence records that the certification process was performed.

*1) Technical Evidence:* In *Proof-Carrying Code (PCC)* [8] techniques, typically the producer himself is the certification body that carries out a formal proof of correctness wrt. some property. The certificate is made up of certain parts of the proof, which a certificate checker may use at any time to formally prove correctness wrt. the same property faster. All PCC techniques are tamper-proof, the certificate check always fails if the property is invalid and the check is correctly implemented. PCC techniques like [9] allow to fully automatically apply the PCC principle. Like the original approach [8], most of the approaches deal with functional properties. For dedicated non-functional properties, PCC approaches for software [10] and hardware services [11] exist.

*Remote Attestation* [12] is used to ensure the integrity of code running on a remote system, the (partial) state of a remote system, or even its behavior. To prove integrity, the remote system (the certificate body) provides collected evidence, e.g., monitoring information, information about the state or cryptographic hashes of those information. A certificate checker, e.g., the user who executes his code on a remote system, investigates if the received evidence matches its expectations.

*Digital Certificates* [13], which are based on cryptographic signatures, are a technique to ensure code or data integrity. A very prominent example are hash values to check the data integrity after a download. Digital certificates are also used for authentication and identification. For example, on GitHub [14], secure shell (SSH) in combination with passphrases are used for authentication, whereas Android APKs must be signed to identify the originator.

*Certifying Algorithms* [6] add to the result of a computation information, which witnesses the correctness of the result. Instead of certifying the result, computation certification [7] certifies the integrity of the computation. Next to the result, checkpoints such as intermediate states of the computation are returned. A certificate checker can parallelly compute for each checkpoint the subsequent checkpoint and check if the computed checkpoint is identical with the provided one.

Damiani et al. [15] propose *Web Service Certificates*. Their idea is to attach a test set for a (non-)functional property to a web service. To validate the correctness of the web service wrt. the property, the certificate checker may execute the tests. Alternatively, a third trusted authority may run the tests and provide a signed document summarizing the test result. For this alternative, Damiani et al. [16] present an approach that constructs a certificate for a service composition on the basis of the test-based certificates of all single services in the composition.

*2) Documentary Evidence:* To ensure reliability, Buckley et al. [17] propose pattern-based reliability certification which combines certification with monitoring. Given a reliability property plus a reliability pattern, the certification body checks if the pattern matches the property. If this is true, he adds a set of monitoring rules, each consisting of a description and a reference to a standard toolkit to monitor the corresponding metric. Thus, the monitoring rules allow to validate if the implemented service complies to the reliability pattern. A trusted certificate checker applies the monitoring rules during execution of the service to validate the reliability property. Ardagna et al. [18] combine certification and monitoring in the context of dependability certification. Based on an initial model-based prediction (a Markov model), they certify the dependability of a service for a fixed amount of time. Thereafter, an (automatic) recertification becomes necessary. When monitoring of the service execution reveals that the service currently does not fulfill the certified property, the certification body tries to downgrade the certificate, i.e., it tries to grant a certificate for a dependability policy which is derived from the original one via relaxation of some of the policy conditions. If the downgrade fails, the certificate is revoked. Note that when the real behavior again matches the originally certified property, the downgrade or revocation will be undone. The approach can also be applied to service compositions.

A common form of documentary evidence is a *Seal of Approval*. Next to the seal, a certification document is often available. The *StarAudit* [19] certificate for cloud service providers belongs to this category. To be certified, an independent certification body, an organization or an accredited auditor, performs an audit in which the offered infrastructure as a service, platform as a service, and software as a service are evaluated according to a publically available catalog of criteria. Depending on the results of the audit, either a certificate for one of three trust levels is issued for two years or no certificate is issued. The certificates are valid only if they are published on the StarAudit website. In contrast to StarAudit, the level of the *Security, Trust & Assurance Registry (STAR)* [20] certificate offered by the cloud security alliance depends on how the certification process is performed. The lowest level uses self assessment. The cloud provider must only provide a report that documents the compliance. The highest level requires continuous auditing. The specialty behind the *Certified Cloud Service* [21] seal offered by the German *Technischer Überwachungsverein (TÜV)* is that although the certificate is granted for three years, compliance is checked once a year and if compliance is no longer given the certificate is revoked. In the context of cloud services, relative documentary evidences such as a ranking of a set of cloud storage providers [22] also exist.

Participating in a certain market is sometimes also a kind of certificate if the goods or the producer must fulfill certain requirements for participation in the market. For example, in the Apple Store each app provided for download passed a review [23] that it adheres to various guidelines.

Furthermore, the quality management processes of many of today's companies are certified to be compliant with the International Organization for Standardization (ISO) 9001 standard. In the certification process, an external certification body performs an audit including interviews with employees and reviews of documents [24]. Additionally, after passing a dedicated exam, people can get a document, a certificate, that they are experts in the corresponding domain. For example, consider the Amazon web service certificates [25], which are valid for two years.

On the basis of the reviewed certification approaches, next we introduce a taxonomy for certificates.

## III. Thoughts on a Taxonomy for Certificates

The goal of our taxonomy is to enable the comparison and ranking of certificates that are issued for the same scope. To that end, we identified four different characteristics.

The first criterion is the *type* of a certificate. Like in the previous section, we distinguish between two types of certificates: technical evidence and documentary evidence. Certificates that are technical evidence carry machine processable information needed by an algorithmic certificate checker to investigate whether the certification criteria are met. In contrast, documentary evidence records that the certification body performed the certification process. Typical examples are seals, badges, and documents.

The second criterion is the *duration* of the validity of a certificate. For example, certificates of the technical evidence type are always valid wrt. the certified entity. Their duration is unlimited. The duration of documentary evidence may either be limited or unlimited. Often, a limited duration corresponds to a time limit [19] [20] [21] [24] [25]. However, we are aware of one approach [18] in which the duration additionally depends on the momentary status of the certified entity.

The next criterion, *quality assurance*, describes how precisely a certificate reflects the adherence of the certified entity to the certification criteria. A *dichotomous quality assurance* means that the certificate either does or does not guarantee the adherence, whereas a *gradual* quality assurance expresses that the certified entity adheres only up to a certain level to the criteria or the complete entity is not checked (e.g., only a test set is executed on the service implementation [15]). A *relative* quality assurance, e.g., a ranking like [22], ranks different certified entities and only describes that the adherence of one certified entity is better than another. If the entity that the certificate is issued for and the entity delivered to the customer are not identical, but the quality check itself is dichotomous, gradual or relative, we say that the quality assurance of the certificate for the delivered entity is *projected* dichotomous, gradual or relative.

The last criterion refers to the existence of a *countercheck*, i.e., whether it is possible for the certificate checker to check that the certified entity adheres to the certification criteria. The information carried by a technical certificate, e.g., a mathematical proof [8], a cryptographic hash [13], monitored data [12], or a test suite [15], naturally imposes such a countercheck. Counterchecks for certificates based on documentary evidence include monitoring [17] [18] or sample examination. Table I gives an overview of the approaches discussed in Section II-B and their classification.

We continue with a detailed motivation for certification in service markets.

## IV. ON SERVICE QUALITY IN SERVICE MARKETS

One underlying characteristic of service markets is that heterogeneous products, i.e., different implementations of the same service but, for example, with diverse non-functional properties are offered. Without further information about a service implementation, service markets, as well as any market for experience goods, face the problem that before the purchase producers, the developers, in the case of service markets, and customers have different levels of knowledge about the service implementation's functional and especially non-functional properties. This constellation is called information asymmetry and arises whenever a product or service is traded whose full characteristics are revealed to the customer only after he bought and experienced it.

Information asymmetry is one reason why high-quality products are driven out of the market in market constellations *without signals* such as customer reviews, which reflect the product quality [2]. The reason is that developing a service implementation with better (non-)functional properties, e.g., a better performance, is typically more expensive. High-quality developers set higher prices to cover their expenses. However, without the revelation of the service quality low-quality developers may also set the same price to increase their profits. Customers who are aware of different quality levels do not trust the developers and show a lower willingness to pay these higher prices. Hence, the prices decrease, high-quality developers cannot cover their expenses and they go bankrupt. In contrast, low-quality developers can cover their expenses with low market prices and remain in the market whereby high quality is finally driven out of the market.

In addition, online service markets have to deal with two further characteristics. First, there is a high fluctuation of service providers, i.e., there are numerous developers which enter and leave the market at any time. Second, often various services are composed to sell a complete software solution.

These characteristics may cause problems even in service markets with an *existing reputation system* especially when new developers enter the market. First, the developers face the moral hazard problem since they can deceive their customers without fearing any sanctions. They can claim to sell an efficiently working service with an appropriate price although their services are working inefficiently. Obliging customers, who buy these services because they are cheap, will be unsatisfied and leave the market for future purchases of services due to this so called adverse selection [26]. Second, the developers indeed offer a high-quality service, but because they have no positive reputation, potential buyers are not willing to pay the demanded price. Hence, the suppliers have two options: 1) They can reduce their prices and invest in a reputation or 2) they can leave the market. Neither of these alternatives is desirable since one party is unsatisfied. In addition, when single services are combined into software packages, customers are hardly enabled to review the single components. Hence, reviews are written for the whole composition and it is difficult to establish reputation for single services since these reviews must be disaggregated to assess the single services.

To overcome these likely occurring problems, information signals on quality can be induced into the market. There are two ways to provide this information: signaling and monitoring. *Monitoring* is the most often used approach in online markets. Customers who already have experienced the seller's service write a review and in this way monitor the observed quality. The purpose of this approach is to build up trust [27]. As already stated above, this approach comes along with problems, in particular for new market participants. This is a severe disadvantage especially in markets for service compositions without few 'big players' but with numerous small and specialized service developers.

The second approach is for the seller to *signal* the quality by showing his trustworthiness. This can be implemented by offering warranties, presenting satisfaction guarantees, or testing the product by a third party and receiving a certificate in return [28]. In markets for service compositions, the signaling approach has weighty advantages: 1) New market participants can reveal the true quality of their services from the beginning. 2) The costs for signals are borne individually by the service developers. 3) The necessity of the disaggregation of customer ratings is removed: The above-mentioned problem of disaggregating customer reviews to assess the single services is bypassed when the quality is signaled by every single developer.

Table I. CLASSIFICATION OF EXISTING CERTIFICATION APPROACHES ACCORDING TO OUR PRELIMINARY TAXONOMY

| Approach | Type | Unlimited Duration | Quality Assurance | Countercheck |
|---|---|---|---|---|
| Amazon Web Service Certificate [25] | documentary | × | gradual | × |
| Apple Store App [23] | documentary | ✓ | gradual | × |
| Certified Cloud Service [21] | documentary | × | gradual | × |
| Certifying Algorithm [6] | technical | ✓ | dichotomous | ✓ |
| Computation Certification [7] | technical | ✓ | dichotomous | ✓ |
| Dependability Certification [18] | documentary | × | gradual | ✓ |
| Digital Certificate [13] | technical | ✓ | dichotomous | ✓ |
| ISO 9001 [24] | documentary | × | gradual | × |
| Pattern-Based Reliability Certification [17] | documentary | ✓ | gradual | ✓ |
| Proof-Carrying Code [8] | technical | ✓ | dichotomous | ✓ |
| Ranking | documentary | ? | relative | × |
| Remote Attestation [12] | technical | ✓ | dichotomous | ✓ |
| STAR [20] | documentary | × | gradual | × |
| StarAudit [19] | documentary | × | gradual | × |
| Top Developer Award | documentary | ? | gradual | × |
| WS-Certificate [15] | technical | ✓ | gradual | ✓ |

These advantages show the potential of certificates in service markets although they come along with the challenges we address in the next section.

## V. Challenges for Certification in Service Markets

On-the-fly markets challenge the use of standard certification techniques. For instance, offered services, the market itself, and also market participants are heterogeneous. Thus, services with technical certificates compete or even interoperate with services provided by companies with a certified workflow. Also, solutions to a user request, the (composed) service plus the execution environment, are created on-demand and hence challenge the creation of certificates in time. Addressing these and further issues in this chapter, we show future directions of research on certification in on-the-fly markets.

### A. *Composition of Certificates*

At the core of on-the-fly computing is the configuration of service compositions out of existing services. Certification must be become *compositional*. First, it is important to find out which types of certificate criteria are compositional at all, e.g., expected runtime might not be compositional if services generate unusual data with a high probability. Second, certification processes for compositional properties must be defined. This is especially interesting for the certification of functional properties. Important questions to answer include whether service compositions can be certified only if all services used have a special technical certificate and how to define technical certificates for models of service compositions. Considering the limited duration of certificates, procedures have to be defined to deal with a composition of certificates when for a subset of services the certificates are expired. This is even more important when the expiration is not necessarily a consequence of time-limited validity but also of varying service quality. A third issue addresses the customers' perception of certificates from different sources. If customers trust different certificates (e.g., those with technical and documentary evidence) differently this must be taken into account since certificates for compositions might not lead to trust though most of the services are certified with trust-building certificates.

### B. *On-the-Fly Certification*

In on-the-fly markets, user requests are not known in advance and often a request must be served, which has not been entered into the market before. In this case, a new solution must be created for the user request. Simultaneously, the newly created solutions must be certified. Typically, issuing a certificate is laborious, e.g., resource and time consuming. The high costs, especially a high issuing time, conflicts with an on-the-fly offer of a solution, i.e., a user gets an offer after a few seconds of his request. Thus, one must rethink the certification process to reduce the certification effort of the new solution, a (composed) service plus the execution environment. An important question is which tasks of the certification process can be done offline in advance. For example, to certify worst case execution time, the worst case execution time of single services can be computed in advance for the available processor architectures in the market. To certify the new solution, one can treat the single services in the composition as a black box considering the worst-case execution time corresponding to the processor architecture that the service will run on. Thus, one only needs to analyze the paths of the composition.

### C. *Business Secrets*

Certificates disclose attributes of the underlying service, which may conflict with business secrets. Composing multiple certified services scales up this problem since two sources of information are supplied with each service. A certified composition of services likely reveals information about the composition process performed by a so called on-the-fly provider and about the single services constructed by several service providers. More importantly, service providers must grant on-the-fly providers, potential competitors in the market, sufficient insights into their single services for certification of the composed service. Moreover, certificates are not checked by the customer himself, but by third entities such as compute centers or on-the-fly providers.

### D. *Economic Perspective*

Certification is tied to costs and benefits in consequence of the reduction of information asymmetries and the customers' higher willingness to pay. In conventional market situations this value is easy to evaluate by comparing certified products with non-certified ones. Hence, suppliers will bear the costs of certification if benefits exceed them. In markets for composed services with compositions including different types of certificates, this suppliers' trade-off is much harder to handle since benefits can hardly be estimated. Mechanisms must be found to predict suppliers' benefits and to distribute them among the single suppliers. This is even more difficult as different certificates with different signal power and costs are employed.

### *E. Realization of Certification*

To integrate certification in distributed service markets such as on-the-fly markets, one must make several design decisions. First, one must choose how to realize the certification bodies. A certification body could be just a service offered by the market infrastructure or it could become a profit-oriented market participant. In the latter case, one must deal with strategic behavior of the certification bodies. For example, they may be corrupt and grant a certificate although the certified entity does not meet the certification criteria, or they may offer certificates ensuring insignificant properties. Second, it must be specified who defines the scope of certification, i.e., the certification criteria, the certification scheme, and so on. For example, one could use a consortium of the market participants or certification bodies can decide themselves. These decisions are important since they have strong and direct implications on the whole market. Other design decisions relate to contracts, penalties for misuse of certificates, or dealing with customer complaints regarding certificates.

### *F. Certification Impact on Service Markets*

So far, certificates are perceived as add-ons to single services. It is unclear whether a *certification system* in the sense of a centralized reputation system (as described in [29]) has implicit consequences on the market functionality. The quality of offered services might be affected and therefore also the market prices. The dynamics of these effects on entities, services, compositions, or participants are unclear. In addition, certificates can be considered as entry requirements on some markets, e.g., the Apple app store, as every app is checked by Apple before it is listed in the store, whereas an app does not need to have any certificate to be published in Google's Play Store. Hence, a high weight of certificates, such as an entrance requirement in the Apple store, might also distinguish different markets (not only apps or services) from each other. Further, interactions of certification systems, e.g., with present reputation systems need to be investigated. It is not certain whether these systems address different dimensions of service attributes or not and, hence, whether these systems are complements or substitutes.

## VI. Conclusion

We presented the necessary ingredients for certification, reviewed existing certification approaches, and classified them according to our taxonomy. Additionally, we motivated the need for certification in service markets and discussed open problems wrt. their usage.

## Acknowledgements

This work was partially supported by the German Research Foundation (DFG) within the Collaborative Research Centre "On-The-Fly Computing" (SFB 901).

## References

[1] Wikipedia, The Free Encyclopedia, "Certification," 2017, https://en.wikipedia.org/wiki/Certification [retrieved: 01-10-2017].

[2] G. A. Akerlof, "The market for "lemons": Quality uncertainty and the market mechanism," The Quarterly Journal of Economics, vol. 84, no. 3, pp. 488–500, 1970.

[3] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," Commun. ACM, vol. 43, no. 12, pp. 45–48, 2000.

[4] M. van der Schaar and S. Z. Zhang, "A dynamic model of certification and reputation," in EC '14, pp. 967–968, ACM, 2014.

[5] ISO, "Certification," 2017, http://www.iso.org/iso/home/standards/certification.htm [retrieved: 01-10-2017].

[6] R. McConnell, K. Mehlhorn, S. Nher, and P. Schweitzer, "Certifying algorithms," Computer Science Review, vol. 5, pp. 119–161, 2011.

[7] S. M. Khan and K. W. Hamlen, "Computation certification as a service in the cloud," in CCGrid '13, pp. 434–441, IEEE, 2013.

[8] G. C. Necula, "Proof-carrying code," in POPL '97, pp. 106–119, ACM, 1997.

[9] M.-C. Jakobs and H. Wehrheim, "Certification for configurable program analysis," in SPIN '14, pp. 30–39, ACM, 2014.

[10] K. Crary and S. Weirich, "Resource bound certification," in POPL '00, pp. 184–198, ACM, 2000.

[11] T. Wiersema and M. Platzner, "Verifying worst-case completion times for reconfigurable hardware modules using proof-carrying hardware," in ReCoSoC '16, pp. 1–8, June 2016.

[12] G. Coker, J. Guttman, P. Loscocco, A. Herzog, J. Millen, B. O'Hanlon, J. Ramsdell, A. Segall, J. Sheehy, and B. Sniffen, "Principles of remote attestation," Int. J. Inf. Secur., vol. 10, no. 2, pp. 63–81, 2011.

[13] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.

[14] "Ssh passphrase on github," 2017, https://help.github.com/articles/working-with-ssh-key-passphrases/ [retrieved: 01-10-2017].

[15] E. Damiani, N. E. Ioini, A. Sillitti, and G. Succi, "Ws-certificate," in 2009 Congress on Services - I, pp. 637–644, IEEE, 2009.

[16] M. Anisetti, C. A. Ardagna, and E. Damiani, "Security certification of composite services: A test-based approach," in ICWS, pp. 475–482, IEEE, 2013.

[17] I. Buckley, E. B. Fernandez, M. Anisetti, C. A. Ardagna, M. Sadjadi, and E. Damiani, "Towards pattern-based reliability certification of services," in OTM '11, pp. 560–576, Springer, 2011.

[18] C. A. Ardagna, R. Jhawar, and V. Piuri, "Dependability certification of services: a model-based approach," Computing, vol. 97, no. 1, pp. 51–78, 2015.

[19] EuroCloud, "Staraudit," 2017, https://staraudit.org/ [retrieved: 01-10-2017].

[20] C. S. Alliance, "Security, trust & assurance registry (STAR)," 2017, https://cloudsecurityalliance.org/star/ [retrieved: 01-10-2017].

[21] TÜV, "Certified cloud service," 2017, http://www.tuv.com/cloud/ [retrieved: 01-10-2017].

[22] PCWELT, "Ranking cloud storage," 2017, http://www.pcwelt.de/ratgeber/Onlinespeicher-ohne-NSA-Die-besten-kostenlosen-Cloudspeicher-in-Deutschland-Schweiz-9829982.html [retrieved: 01-10-2017].

[23] A. Inc., "App review," 2017, https://developer.apple.com/app-store/review/guidelines/ [retrieved: 01-10-2017].

[24] ISO, "ISO 9000—selection and use," 2009, ISO Technical Committee ISO/TC 176.

[25] Amazon, "Amazon webservice certification," 2017, https://aws.amazon.com/certification/ [retrieved: 01-10-2017].

[26] G. Lewis, "Asymmetric information, adverse selection and online disclosure: The case of ebay motors," The American Economic Review, vol. 101, no. 4, pp. 1535–1546, 2011.

[27] P. Resnick and R. Zeckhauser, "Trust among strangers in internet transactions: Empirical analysis of ebays reputation system," The Economics of the Internet and E-commerce, vol. 11, no. 2, pp. 23–25, 2002.

[28] D. Dranove and G. Z. Jin, "Quality disclosure and certification: Theory and practice," J. Economic Literature, vol. 48, no. 4, pp. 935–963, 2010.

[29] S. Brangewitz, A. Jungmann, R. Petrlic, and M. Platenius, "Towards a flexible and privacy-preserving reputation system for markets of composed services," in SERVICE COMPUTATION '14, pp. 49–57, IEEE, 2014.