DOES PAIN RESULT IN GAIN? ASSESSING CLOUD SERVICE CERTIFICATIONS' EFFECTIVENESS

Research-in-Progress

Jens Lansing
Faculty of Management,
Economics and Social Sciences
University of Cologne
Albertus-Magnus-Platz,
50923 Cologne, Germany
lansing@wiso.uni-koeln.de

Ali Sunyaev
Faculty of Management,
Economics and Social Sciences
University of Cologne
Albertus-Magnus-Platz,
50923 Cologne, Germany
sunyaev@wiso.uni-koeln.de

Abstract

Cloud service certifications (CSCs) gain increasing attention in practice as a measure against the prevailing uncertainties of cloud computing, but demand efforts for passing audit requirements. However, research findings on certifications' effectiveness are inconclusive. This research-in-progress paper develops a research model to evaluate CSCs' effects on two certification outcomes suggested by trust theory and signaling theory - trust and price premiums - while also accounting for trust in certification authority, reputation, personal relevance of using cloud services and self-provided assurance statements. Compared to extant research on certifications, which primarily focuses on privacy and security in e-commerce, CSCs address a novel product category and provide assurances beyond privacy and security, such as availability and interoperability. Furthermore, by investigating price premiums, we focus on a widely neglected certification outcome. Thus, we expect our model to contribute to a deeper understanding of the contextual conditions under which certifications are effective signals and trust-assurances.

Keywords: Cloud Computing, Cloud service certification, trust, signaling, price premiums

Introduction

Cloud service certifications (CSCs) recently were declared a key action of the European Union's cloud computing strategy (European Commission 2012) and various certification programs are emerging, such as Cloud Security Alliance STAR and TRUSTe Cloud Data Privacy Certification. Though consumers are expected to store more than a third of their personal data in the cloud by 2016 (Gartner Research 2012), they still face uncertainties concerning for instance security, privacy and vendor lock-in (Li and Chang 2012). Through the lens of signaling theory, CSCs serve as a signal of unobservable quality of a cloud service and its provider (Kirmani and Rao 2000). From a trust theory perspective, CSCs are a set of third-party "trust-assuring arguments" that engender trust (Kim and Benbasat 2009). Because both signals and trust mitigate uncertainty (Pavlou et al. 2007), the emergence of CSCs can be interpreted as a measure against the prevailing uncertainties of cloud computing (Sunyaev and Schneider 2013). However, certification demands significant efforts from providers, including passing an audit, implementing organizational changes and paying certification fees. Surprisingly, despite calls for developing (European Commission 2012; Khan and Malluhi 2010) and investigating the efficacy of certifications in the cloud computing context (Venters and Whitley 2012), research on the outcomes of CSCs is scarce.

Tough IS research investigated certifications utilizing both signaling theory and trust theory, a clear understanding of certification outcomes and facilitating conditions for these outcomes is still lacking. Signaling theory suggests that a certified firm can offset costs of acquiring a signal such as a CSC by pricing a premium (Gopal and Gao 2009; Spence 1973). For example, Mai et al. (2010) find that privacy seal-bearing e-commerce vendors charge a price premium. However, only few other studies investigate certifications' direct effect on prices. Furthermore, IS research has intensively studied certifications' effects on trust in e-commerce, but with inconclusive results (Hu et al. 2010). For example, Kim and Kim (2011) find a significant effect of certifications on trust, whereas McKnight et al. (2004) do not. Recently, Kim and Benbasat (2009) found that certifications' effects on consumers' beliefs, attitudes, and behaviors not only differ by contextual factors, such as product or service type, price, and personal relevance, but also by a certification's content and source. Thus, a certification will only be effective if its content is properly designed for a specific product or service type and if it is issued by a trustworthy source.

This research-in-progress designs a CSC and evaluates its effectiveness in terms of two outcomes suggested by signaling theory (price premium) and trust theory (trust), addressing the research question: *Do CSCs increase users' trust in and are users willing to pay a price premium for unknown, but certified cloud services?* To answer the research question, this paper builds on a previous study in which we identified and conceptualized ten assurances of CSCs based on expert interviews, existing CSCs and literature as well as empirically assessed their relative importance (cf. Lansing et al. 2013 and below). Results show which assurances are relevant and valued most by consumer cloud service users. Using these assurances as an input, this paper develops a research model and hypotheses and proposes an experimental design for empirical evaluation. To deepen theoretical understanding of facilitating contextual conditions and enhance practical implications, the research model includes two additional signals and trust-assurances: reputation of a cloud service and a self-provided assurance statement (AS) which contains the same ten assurances as the CSC. As the previous study, this study focuses on the consumer context.

We expect our study to provide several research and practical contributions. First, by building on a validated and carefully conceptualized set of assurances for a hitherto unstudied context and evaluating CSCs' outcomes compared to ASs and reputation, our study deepens the understanding of the contextual conditions under which certifications are effective signals and trust-assurances. Second, by focusing on price premiums, our study investigates CSCs' effects on an underexplored certification outcome. Third, IS managers may use our results to decide whether the substantial costs and organizational changes required for certifying with a CSC are sufficiently offset by monetary (price premiums) and non-monetary (trust) rewards compared to the alternative means of ASs and reputation. Last, in combination with our previous study's results, results may guide certification authorities in designing effective CSCs.

The paper proceeds as follows. First, we provide theoretical background on cloud computing and certifications. Second, we present the research model and formulate hypotheses. Third, we outline the agenda for the empirical study, including a brief summary of our previous study and a preview of our experimental design. We conclude with suggestions for future research and potential implications.

Background on Cloud Computing and Certifications

Cloud computing enables "access to a shared pool of configurable computing resources" (Mell and Grance 2011) which are provisioned from large-scale datacenters (the cloud) (Armbrust et al. 2010) over a network. Access is granted on-demand in a self-service manner with minimal provider interaction (Mell and Grance 2011). We name any types of such computing resource cloud service and distinguish infrastructure services, platform services and application services (Mell and Grance 2011). Here, we focus on public cloud computing, which is a model in which the cloud is accessible "for open use by the general public" and operated by a third-party provider (Mell and Grance 2011). We consider a cloud service to be a duality, as it is both an IT artifact and a service provided by provider. In our work we distinguish three roles (cf. Leimeister et al. 2010): cloud service providers are organizations that provide a cloud service, cloud service users are individuals that use a specific type of cloud service, and cloud marketplaces are intermediaries that categorize cloud services and support cloud service users in choosing a service.

CSC refers to a process in which a cloud service provider's processes and services are evaluated against a predefined set of criteria via an audit by a third party, which formally acknowledges that the standard defined by the criteria is met (Sine et al. 2007). Signaling theory (Spence 1973) suggests that in markets with information asymmetries, signals may reduce related uncertainties by providing information on unobservable attributes of another party. Certifications are thus signals because the audit required for a certification reveals information about these attributes. Within the logic of signaling theory, costs for acquiring a signal (e.g., needed changes to fulfill a certification's requirements) are lower for high-quality firms than for low-quality firms, which will prevent the latter from seeking certification (Gopal and Gao 2009). Extant research on certifications utilizing signaling theory predominately focuses on certifications' effects on certified firms. For example, a capability maturity model (CMM) certification leads to increased export revenues, which are implicitly assumed to be caused by a price premium for the reduced information asymmetries due to the CMM's quality signal (Gao et al. 2010). From a consumer's perspective, a certification allows consumers to discriminate high-quality from low-quality firms, thereby influencing a consumer's beliefs, attitudes and behaviors (Kimery and McCord 2006). Empirical studies find certifications to influence willingness to provide information to a e-commerce vendor and trust (Aiken 2006; Wang et al. 2004). Kimery and McCord (2006) find consumer's understanding of e-commerce certifications content is incomplete or in some areas inaccurate and certifications often are unnoticed, which questions a certification's signaling ability in that particular context.

Trust between buyers and sellers in the e-commerce domain has been the major focus of IS research on certifications and seals. Trust is "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" (Rousseau et al. 1998). McKnight et al. (2002) break down trust into trusting intention, which "means the truster is securely willing to depend, or intends to depend, on the trustee", and trusting beliefs, which "means the confident truster's perception that the trustee [...] has attributes that are beneficial to the truster." Predominantly investigated certifications are information privacy (e.g., Hui et al. 2007), information security (e.g, Kimery and McCord 2006), online vendor's integrity or reliability (e.g., Zhang 2005), or combinations of those (e.g., Hu et al. 2010). However, empirical findings on the effect of certifications on trust so far have been inconclusive (cf. Hu et al. 2010 and Lowry et al. 2012 for comprehensive overviews).

As stated above, the effect of trust-assuring arguments such as certifications on trust depends on the argument's content and source as well as contextual factors influencing consumers' perceptions of the argument (Kim and Benbasat 2009). In terms of content, research finds that a trust-assuring argument's influence on trusting beliefs is contingent upon the type of argument content and its formulation. For example, combining privacy assurances with security or integrity assurances attenuates the single effect of privacy assurance on trusting beliefs (Hu et al. 2010). Furthermore, trust-assuring arguments lead to higher increases in trusting beliefs when the argument's claims are supplemented by data as grounds for a claim and backings for "why data should be accepted" (Kim and Benbasat 2006). In terms of source, a certification may foster trust transference (cf. Doney and Cannon 1997). Assuming a consumer perceives a certification authority as trustworthy, a certification may establish a cognitive association between a certified provider and a certification authority, by which a consumer's trust in the certification authority is transferred to the certified provider. For example, Nöteberg et al. (2003) find that assurances provided by a third-party certification lead to lower privacy and integrity concerns than vendor-provided assurances, but do not find any significant differences between different third-party assurance providers. Last, contextual contingency factors, such as vendor and product familiarity, product category and consumer involvement, influence a certification's effect on trust. Mauldin and Arunachalam (2002) only find a significant effect of assurance seals on purchase intentions if product familiarity is low and disclosures of a retailer's business practices are not observed. Zhang (2005) finds that reliability assurance seals increase willingness to buy for both commodity and experience goods, but information assurance seals only increase willingness to buy for commodity goods. Kim and Kim (2011) find that a well-known privacy seal only engenders trust in unfamiliar vendors if involvement is low.

In sum, certifications may engender trust and signal quality under the following conditions: First, assurances conveyed by certifications need to be meaningful to users and need to address concerns relevant for the product category. Second, assurances need to influence trusting beliefs. Finally, the authority that issues the certification needs to be perceived as trustworthy. As discussed, we already investigated the first condition in a prior study and conceptualized assurances that are relevant and meaningful to consumer cloud service users (Lansing et al. 2013). Next, we focus on the second and third condition and experimentally evaluate a certification that conveys these assurances and that is issued by a trustworthy source while controlling for contextual factors. The scope of the study is to evaluate a CSC that comprises all ten conceptualized assurances. Future research may then build upon the results and study different CSC designs (e.g., comparing subsets of the ten assurances; cf. final section).

Research Model and Hypotheses

We draw on and extend Ba and Pavlou's (2002) model on the effect of reputation on trust and price premiums (Figure 1). Following trust theory, initial trust (i.e., trust in a third party without a prior relationship) is built through cognitive processes that influence trusting beliefs by processing available information and cues (McKnight et al. 1998), such as certifications and reputation. Thus, we posit that trusting beliefs in a cloud service are explained by presence of a CSC (H_{1a}), trust in a certification authority (H_{1b}), and reputation (H_2), and the increased trust leads to price premiums (H_4) moderated by personal relevance of using a cloud service (H_5). We further posit that presence of self-proclaimed assurance statement (AS) including the same assurances as a CSC influences trusting beliefs in a cloud service (H_3). The latter is intended as a comparison to verify whether it is our designed CSC that influences trusting beliefs and price premiums or the mere statement of assurances. Although we are interested in the effect of CSCs on trust in a cloud service, other antecedents of trust need to be controlled because an isolated investigation of trust antecedents might be misleading (Li et al. 2008). We control for the well-established initial trust antecedents disposition to trust and institution-based (Li et al. 2008; McKnight et al. 2002). Furthermore, we control for technology acceptance constructs perceived ease of use and perceived usefulness because trusting and paying for a cloud service implies acceptance and both constructs interact with trusting beliefs (Gefen et al. 2003; Wang and Benbasat 2005). Last, we control for knowledge (expressed by internet experience, cloud usage experience and general knowledge about cloud services).

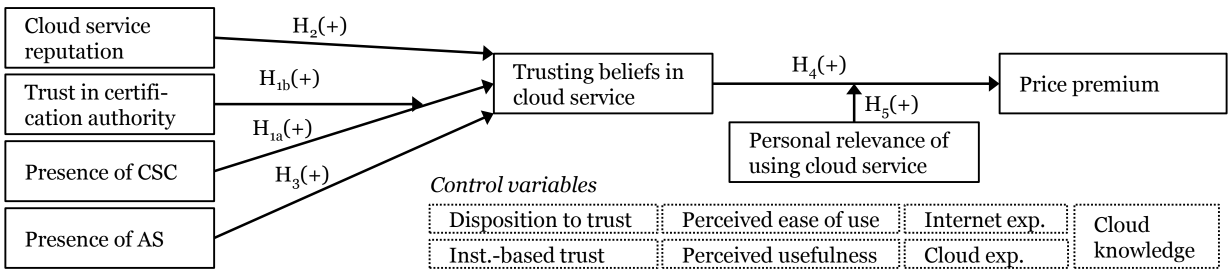

Figure 1. Research Model

Following our notion that a cloud service is inseparably an IT artifact and a service provided by a cloud service provider, trusting beliefs in a cloud service could be shaped by attributes of the cloud service provider or attributes of the IT artifact. Extant research supports both perspectives (e.g., trusting beliefs in an IT outsourcing provider (Lee and Choi 2011) and trusting beliefs in an IT artifact (McKnight et al. 2011; Wang and Benbasat 2005) and suggests that both types of beliefs are discriminant, but complementary (Lankton and McKnight 2011; Li et al. 2009). Hence, trusting beliefs in a cloud service means that one believes the cloud service provider and the cloud service IT artifact have favorable attributes.

Trusting beliefs in a cloud service deal with the cloud service user's beliefs in specific attributes of the provider, e.g. competence, benevolence and integrity (Mayer et al. 1995), and of the technology, e.g., functionality, reliability, or helpfulness (McKnight et al. 2011). Cloud services are purchased via self-service mechanisms over the internet (Mell and Grance 2011) and the interior processes of a cloud services are opaque to the user. Available information on the cloud service is restricted to information provided by cloud service providers via the provider's website or by cloud service marketplaces (e.g., Google Apps Marketplace (Google 2012)). Thus, when first evaluating an unknown cloud service, a user only has little information to cognitively process attributes of the cloud service and the provider. A CSC provides proofed information that the provider and the technology fulfill specific quality criteria. Hence, a CSC contains information about a provider's competence and integrity, as well as capability and reliability of the service technology that can be processed by trust-building cognitive processes. In sum, we posit:

H_{1a}: Presence of a CSC will positively influence a consumer's trusting beliefs in a cloud service.

Extant research notes that any institutional trust producing mechanism needs to be socially legitimized (Zucker 1986). Legitimization of a certification may arise from a reputable authority that issues the certification. Given these conditions, presence of a CSC may initiate a trust-transference process (cf. Doney and Cannon 1997) from a certification authority (i.e., a CSC's source) to a cloud service and its provider. This relationship implies that a customer will not only trust a cloud service because of certified service quality (i.e. the CSC's content), but also because of an implicit endorsement of the service by a certification authority. Empirical research in e-commerce demonstrates that certifications engender trust both through the provided assurances and trust in the certification authority (Kaplan and Nieschwietz 2003), but does not explicitly investigate interactions. Reflecting on Kim and Benbasat's (2009) finding that (all else equal) trust-assuring arguments by a third-party (high source trust) have a higher effect on trusting beliefs than trust-assuring arguments provided by a web vendor (low source trust), we posit:

H_{1b}: Trust in certification authority moderates the effect of presence of CSC on trusting beliefs in a cloud service. Presence of CSC will elicit greater trusting beliefs in a cloud service if trust in certification authority is high than if trust in certification authority is low.

Reputation refers to "the extent to which firms and people in the industry believe a supplier is honest and concerned about its customers" (Doney and Cannon 1997). Initial trust develops through processing cognitive cues, such as first impressions, reputation and stereotypes, and thus does not require long-term personal interactions (McKnight et al. 1998). Reputation influences initial trust as it provides second-hand information on the service's trustworthiness, i.e., is a proxy for process-based trust (Zucker 1986). Thus, other users' perceptions that a cloud service is trustworthy provide additional information to evaluate trustworthiness of a cloud service and a cloud service with a high reputation is likely to be perceived more trustworthy. Previous research finds a positive influence of reputation on trust in an IT service provider (Lee et al. 2008) and in a technology (Li et al. 2008). Thus, we hypothesize:

H_2: Reputation has a positive influence on a consumer's trusting beliefs in a cloud service.

An AS is a set of trust-assuring arguments supplied by a cloud service provider consisting of claims and "supporting statements [...] to address trust-related concerns" (Kim and Benbasat 2006). Compared to a CSC, an AS provides the same content, but has a different source. By posting an AS, a cloud service provider is "publicly committing to some level of assurance" (Lowry et al. 2012). Thus, an AS provides cognitive cues on a provider's competence and integrity, as well as technology functionality and reliability. ASs have been found to influence trusting beliefs in a web vendor (Kim and Benbasat 2009) and perceived assurance, which is a trust antecedent (Lowry et al. 2012). We thus hypothesize:

H_3: Presence of an AS has a positive influence on a consumer's trusting beliefs in a cloud service.

Cloud service users have few means to assess a cloud service's quality before usage (Sunyaev and Schneider 2013). Cloud service users may only gain experience and knowledge on a cloud service by using it over a longer period of time, but even then, users do not have a guarantee on the cloud service provider's behavior or the cloud service technological reliability. In that sense, cloud services are similar to physical products with experience attributes, which are products "whose quality can be determined only after purchase" (Rao and Bergen 1992). Users may store data of varying personal importance within cloud service, such as documents, music, photos and videos, whose loss, unavailability, or leakage is risky for cloud service users. Given this situation, cloud service users may pay providers an additional fee for not taking the opportunity to act opportunistically and for providing a high quality service (Rao and Bergen 1992). We name this additional fee a price premium, which means "the monetary amount above the average price received by [cloud service providers] for a certain matching [cloud service]" (Ba and Pavlou 2002). From a signaling theory perspective, a certified provider may also offset costs of acquiring a signal such as a CSC by pricing such a premium (Gopal and Gao 2009; Spence 1973). Because trust mitigates uncertainties related to online mediums (Pavlou et al. 2007), cloud service users that have high trusting beliefs in a cloud service (e.g., due to a CSC, an AS or high reputation) are more likely to perceive to be less exposed to transaction and product uncertainties. Thus, cloud services that gain higher trusting beliefs may gain a price premium. For example, e-commerce sellers with higher reputation receive higher trust in their credibility, and gain price premiums (Ba and Pavlou 2002). In sum, we hypothesize:

H_4: Trusting beliefs in a cloud service has a positive influence on price premiums for the cloud service.

Following H_4, providers gain a compensation for reducing transaction and product uncertainties below average and providers that provide a cloud service bearing a higher than average risk receive a price discount (Ba and Pavlou 2002). Hence, the price premium increases with the risk of using a cloud service. In the present context, risk is determined by a cloud service user's dependency on the availability of a cloud services' functionality as well as the personal relevance of data stored within a cloud service. As mentioned earlier, cloud service users may store data of varying personal relevance. Using a service is thus riskier for cloud service users storing data of high personal relevance than for those storing data of low personal relevance. Consequently, cloud service users that store data of high personal relevance seek for more trustworthy providers and are willing to pay a higher than average price. We thus posit:

H_5: Personal relevance of using a cloud service moderates the effect of trusting beliefs in a cloud service on price premiums. Trusting beliefs in a cloud service will elicit higher price premiums if personal relevance of using a cloud service is high than if personal relevance of using a cloud service is low.

Agenda for Experimental Evaluation

The experiment aims at mimicking a choice situation of a self-serviced provision from a provider or from a cloud marketplace. Our experimental design follows Ba and Pavlou (2002), who suggested a within-subject design for evaluating the effect of reputation on trust and price premiums in e-commerce auctions. The design demands participants to first scrutinize different profiles of vendors, then rate trust levels for each profile and finally to enter a price relative to a given mean price for each profile. We adapt this approach by asking participants to only evaluate one profile of a cloud service and introducing three treatments instead of multiple profiles. The experimental setting allows manipulating trust-building cognitive processes that evaluate information contained in each profile by varying presence of a certification (present, not present), presence of an AS (available, not available), and reputation (low reputation, medium reputation, high reputation). However, we omit the treatment that would present a certification and an AS for parsimoniousness, resulting in nine groups. The overall study consists of three phases: (1) compilation of stimulus material, (3) experiment design and pilot study, and (3) main experiment.

Table 1. Information Available to Participants

Type	Stimulus material
Provider	Description, size, revenues, years in cloud business, other cloud services
Cloud Service	Description, features: encryption, file versioning, file sharing (public/private)
Reputation	Approximated by rating: 5 stars (high), 3 stars (medium), 1 star (none/low)
Certification	Assurance claims, description of audit process
Certification Authority	Issuer: description, size, years in business, code of conduct
Assurance statement	Assurance claims (same as certification)

Completed Work: Compilation of Stimulus Material

We already completed the first phase of compiling stimulus material (Table 1) and determining certification assurances (i.e., content; cf. Lansing et al. 2013). We design a novel CSC because current CSC are just emerging and often only include one or two assurances (e.g., Cloud Security Alliance STAR focuses on security, and TRUSTe Cloud Data Privacy Certification focuses on privacy), which contradicts our prior study's finding that consumers also value assurances beyond security and privacy (cf. Lansing et al. 2013 and below). A fictitious CSC further allows ensuring effective formulation of content as proposed by Kim and Benbasat (2006). The presented cloud service is fictitious to ensure participants have no prior experience with the service. We focus on consumer cloud storage services (a contemporary example is Dropbox.com), because these have lower asset specificity than application or platform services and are highly homogenous (see below). Both usage of fictitious certifications and services is common in IS research on certifications and trust (e.g., Kim and Benbasat (2009) and Hu et al. (2010) design fictitious certifications and Lowry et al. (2012) use a fictitious website). To foster trust transference, we will state the CSC is issued by a well-known existing certification authority such as ISO. Reputation is approximated by a 5-star-rating icon, which is a common element of cloud marketplaces such as Google Apps Marketplace (Google 2012).

To increase external validity, profiles of cloud services will reflect existing cloud services. We collected information on 51 consumer cloud storage services and their providers in November and December 2012. Results show that services are interchangeable with regards to major attributes such as encrypted transmission (80%) and storage (78%), file versioning (90%) as well as sharing files with public (98%) and registered users (96%). All services allow access from major operating systems (Windows, MacOSX and Linux) as well as mobile devices (iOS and Android). Using data from Cloud Reviews (2013), we find that services differ only in terms of price and external rating (our proxy for reputation). For the former, prices range between € 0.003 and € 0.615 per GiB per month (median € 0.065, mean € 0.118, standard deviation € 0.139). For the latter, on a 5-point scale, 14% have the lowest rating of 1, 22% a rating of 2, 30% a rating of 3, 19% a rating of 4 and 14% have the highest rating 5. Hence, by focusing on three rating categories in the experiment, we cover the whole bandwidth of cloud services, with each category covering a roughly equal market share. Due to the similarities between services, all profiles in the experiment will be the same (except for treatments) and include the most common attributes as indicated above.

Table 2. Results of BWS Experiment (cf. Lansing et al. 2013)

Assurance	Counting Analysis Scores			Conditional Logistic Regression		Rank
	Mean	Std. Dev.	Skewness	Coefficient	Std. Error	
Privacy	0.63	0.35	-0.74	3.20	0.16	1
Security	0.51	0.33	-0.59	2.85	0.16	2
Availability	0.40	0.37	0.21	2.55	0.15	3
Interoperability	0.08	0.45	-0.42	1.59	0.14	4
Contract	-0.02	0.38	0.25	1.50	0.14	5
Legal	-0.12	0.40	-0.13	1.08	0.13	6
Customer Support	-0.16	0.48	0.26	1.02	0.13	7
Process Maturity	-0.34	0.37	0.03	0.55	0.13	8
Flexibility	-0.42	0.38	0.48	0.37	0.13	9
Financial Stability	-0.56	0.31	0.58	-	-	10

All regression coefficients are significantly different from zero at p<.001, except Flexibility (p<.01)

As outlined, our prior study (Lansing et al. 2013) provides conceptualizations of assurances for CSCs (and ASs) as well as the relative importance of assurances for consumers. Incorporating these assurances ensures satisfying the implicit assumption that a CSC's assurances are relevant and meaningful to users (cf. "Background" section). We followed a four-step approach to determine assurances relevant for CSCs. First, we derived an initial set of assurances from extant literature on certifications. Second, we searched the literature on cloud computing for cloud-specific consumer concerns. Third, to discuss, refine, and above all validate the derived assurances, we conducted 13 expert interviews between June and September 2012. Fourth, we conceptualized the identified assurances and conducted a discrete choice experiment that follows the best-worse scaling (BWS; cf. Finn and Louviere 1992) method to empirically measure consumer's preferences for the ten assurances. Similar to regular choice experiments, respondents in a BWS experiment are repeatedly presented a set of three or more choices. But instead of choosing one option as in regular choice experiments, respondents are asked choose the most preferred *and* the least preferred option. Using observations obtained from all choices of all participants, preferences for each choice option can be calculated by a scoring mechanism or by a conditional logistic regression (Table 2). An in-depth discussion of the BWS method and results is provided in our original paper.

Future Work: Conceptual Development, Pilot Study and Experimental Evaluation

In the second phase, we will design the CSC and AS following Kim's and Benbasat's (2006) guidelines for effective phrasing of trust-assuring arguments. Furthermore, we will develop our measurement instrument based on measurement items from prior research (e.g., Lee and Choi (2011) for trusting beliefs in IT outsourcing providers, McKnight et al. (2011) for trusting beliefs in IT artifacts, Kaplan and Nieschwietz (2003) for trust in certification authority, and McKnight et al. (2002) for disposition to trust and institution-based trust). Next, we will conduct focus group discussions with experienced IS scholars as well as consumer cloud service users to assess clarity of and to collect feedback on stimulus material (Table 1) and the measurement instrument. As a last preparatory step, we will conduct a pilot study with students to evaluate validity and reliability and use results for further refinement following the same procedure as the main study. The pilot study also allows evaluating the set of control variables, which currently is comprehensive because trust is influenced by many factors that may superimpose a CSCs effect (Li et al. 2008; Lowry et al. 2012). Thus, to increase parsimoniousness of model and measurement instrument, we plan to evaluate whether all control variables are necessary.

The main study in the third phase will utilize a web-based questionnaire consisting of four stages. First, participants will be randomly assigned to one of the nine groups and participants are shown information on cloud storage services and CSCs to ensure a common baseline understanding. Second, participants will be asked to answer a pre-experimental questionnaire that captures control variables because these are independent of treatment. The third stage consists of two tasks: elicitation of trusting beliefs and price indication. For the first task, stimulus material will be presented in form of a profile of a cloud service (cf. Table 1) and screenshots of a cloud storage service's functionality. The latter is common in experimental IS research on trust to stimulate perceptions (e.g. Vance et al. (2008) show screenshots of a mobile online shop). The profile includes information on service, service provider, and reputation rating (all groups) as well as an icon indicating either a CSC or a link to a self-proclaimed AS (treatments only). By clicking on the certificate icon or the link for the AS, participants can retrieve the respective trust-assuring arguments. For the CSC, additionally information on the certification authority as well the audit process is provided. To complete the task, participants are asked to indicate trusting beliefs and personal relevance of using the cloud storage service. For the second task, price determination, participants are asked to indicate their willingness to pay for the shown cloud service. To ease procedure, the average price for cloud services is stated (12 ct. per GiB per month) and participants are asked to indicate their willingness to pay as a percentage of the stated average. In the fourth and last stage, participants will be asked additional manipulation check questions. Specifically, we ask to recall the services' reputation and the average price for a cloud service as well as whether participants recognized the given assurance and its source.

We will recruit participants from SoSci Panel which maintains a database of more than 90,000 voluntarily registered consumers from differing age groups and educational backgrounds (SoSci Survey 2013). A recent survey shows that all age groups and educational classes use cloud storage services (Bitkom 2013). Hence, inviting consumers from all age groups should result in a representative sample. Calculating with SoSci Panel's typical response rates of 16-25%, we plan to invite 2,000 consumers, aiming for a sample size of about 400. Because we are interested in the simultaneous effects of treatments and other variables, rather than isolated treatment effects, data will be analyzed by structural equation modeling (SEM) using partial least squares (PLS) and treatments will be included in the model as binary variables as commonly applied in experimental IS research (e.g., Benlian et al. 2012). Following guidelines for PLS-SEM (Hair et al. 2013), the intended sample size should be sufficient for our rather small model.

Suggestions for Future Research and Conclusion

This paper proposes a novel CSC and describes a research model that allows evaluating its effects on two certification outcomes suggested by trust theory and signaling theory – trust and price premiums – while accounting for two other signals – reputation and assurance statement – as well as trust in a certification authority and personal relevance of using a cloud service.

Once confirmed, the research model may serve as a baseline model for future studies on CSCs. As outlined, our previous study (Lansing et al. 2013) informs this study by providing conceptualizations of assurances relevant for cloud computing, thus ensures that conditions for certification effectiveness are satisfied (i.e., assurances are relevant and meaningful; cf. "Background" section). Results of the previous study (Table 2) point out additional research opportunities. For example, negative counting scores indicate which assurances respondents are willing to abandon (Auger et al. 2007). Hence, one might hypothesize that a CSC which only contains assurances with positive scores will lead to increased trusting beliefs and price premiums, whereas a CSC which only contains assurances with negative scores will not. Furthermore, extant research in e-commerce finds attenuating effects between privacy and other certification assurances (Hu et al. 2010). Future studies could investigate whether such mutually reinforcing or attenuating effects of CSCs' assurances on trusting beliefs and price premiums exist. Similarly, future research might investigate possible interactions between ASs and CSCs. To focus on CSCs and to reduce sample size requirements, we limited the current design to direct effects of CSCs and ASs and did not include interaction effects between CSCs and ASs. From a practical perspective, it is also interesting to study whether a CSC's effects on trusting beliefs and price premiums are reinforced or attenuated by an AS. Such interactions between ASs and CSCs could be evaluated by expanding the research design to include three additional treatment groups (i.e., one for each reputation rating) and showing respondents in these groups both a CSC and an AS. Likewise, future research could investigate further interactions between CSCs and reputation than those within this study. Due to the primary focus on evaluating a CSC's outcomes, the current research design is restricted to an unknown certified provider and manipulates reputation by varying the cloud service's rating across groups. Thus, the current design assumes that reputation is based on a cloud service. In practice this assumption holds for providers that offer a single or few cloud services (e.g., Dropbox), but might not hold for providers who provide cloud services as one product among many others (e.g., Google). Here, reputation might be based on overall provider reputation because consumers are not able to differentiate overall provider reputation from the cloud service's reputation. Future studies may investigate whether the effect of CSCs on trusting beliefs and price premiums differs between the two types of cloud service providers and associated reputations by introducing an additional treatment that varies stimulus material on the cloud service provider and by explicitly measuring reputation as a variable (e.g., using measurement items from Li et al. 2008). Finally, we consider testing the model with professional cloud service users a promising research opportunity. Many certifications, such as CMM, are a prerequisite for bidding (Gopal and Gao 2009). Hence, they are not used for signaling high quality but only for appearing legitimate in a market (Gopal and Gao 2009), which undermines one of the basic assumptions for increased trust and price premiums.

In sum, the study responds to calls for developing (European Commission 2012; Khan and Malluhi 2010) and investigating the efficacy of certifications (Venters and Whitley 2012) in the cloud computing context. Particularly in light of the hitherto inconclusive findings on the effectiveness of certifications, empirical validation of the research model will contribute to a deeper theoretical understanding of the contextual conditions under which certifications are effective signals and trust-assurances. As discussed, extant research primarily focused on e-commerce, where certifications address concerns about sellers rather than products sold online, such as security and privacy of transaction data, fears of seller opportunism and information asymmetries (Pavlou et al. 2007). In contrast, a CSC address concerns about a provider *and* a service (i.e., an IT artifact), including service quality, security, privacy, and availability as well as legal compliance and lock-in effects (Armbrust et al. 2010; Marston et al. 2011; Narasimhan and Nichols 2011). Moreover, previously investigated certifications are privacy, security, online vendor's integrity or reliability, or combinations of those, whereas CSCs in this study include additional assurances, such as service availability, interoperability and contract. By measuring trusting beliefs in the provider and the service technology, we also hope to contribute to the growing literature on trust in IT artifacts (Gefen et al. 2008). Finally, by focusing on price premiums in addition to trust, we respond to Gao et al. (2010) and focus on a largely neglected potential certification outcome.

From a practical perspective, implications of our research can help certification authorities to better understand how to design CSCs. Also, our research can inform cloud service providers whether certifying services provides monetary as well as non-monetary value such as trust and how these compare to reputation and self-proclaimed assurance statements.

References

Aiken, K. D. 2006. “Trustmarks, Objective-Source Ratings, and Implied Investments in Advertising: Investigating Online Trust and the Context-Specific Nature of Internet Signals,” *Journal of the Academy of Marketing Science* (34:3), pp. 308–323.

Armbrust, M., Stoica, I., Zaharia, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., and Rabkin, A. 2010. “A View of Cloud Computing,” *Communications of the ACM* (53:4), pp. 50–58.

Auger, P., Devinney, T. M., and Louviere, J. J. 2007. “Using Best–Worst Scaling Methodology to Investigate Consumer Ethical Beliefs Across Countries,” *Journal of Business Ethics* (70:3), pp. 299–326.

Ba, S., and Pavlou, P. A. 2002. “Evidence of The Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior,” (26:3), pp. 243–268.

Benlian, A., Titah, R., and Hess, T. 2012. “Differential Effects of Provider Recommendations and Consumer Reviews in E-Commerce Transactions: An Experimental Study,” *Journal of Management Information Systems* (29:1), pp. 237–272.

Bitkom 2013. *Die Cloud wird zum privaten Aktenschrank*.

Cloud Reviews 2013. *CloudReviews - Cloud Storage Services*. http://www.cloudreviews.com/cat/cloud-storage.html. Accessed 26 February 2013.

Doney, P. M., and Cannon, J. P. 1997. “An Examination of the Nature of Trust in Buyer-Seller Relationships,” *Journal of Marketing* (61:2), pp. 35–51.

European Commission 2012. *Unleashing the Potential of Cloud Computing in Europe*, Brussels.

Finn, A., and Louviere, J. J. 1992. “Determining the Appropriate Response to Evidence of Public Concern: The Case of Food Safety,” *Journal of Public Policy and Marketing* (11:2), pp. 12–25.

Gao, G., Gopal, A., and Agarwal, R. 2010. “Contingent Effects of Quality Signaling: Evidence from the Indian Offshore IT Services Industry,” *Management Science* (56:6), pp. 1012–1029.

Gartner Research 2012. *Gartner Says That Consumers Will Store More Than a Third of Their Digital Content in the Cloud by 2016*. http://www.gartner.com/it/page.jsp?id=2060215. Accessed 13 November 2012.

Gefen, D., Benbasat, I., and Pavlou, P. A. 2008. “A Research Agenda for Trust in Online Environments,” *Journal of Management Information Systems* (24:4), pp. 275–286.

Gefen, D., Karahanna, E., and Straub, D. W. 2003. “Trust and TAM in Online Shopping: An Integrated Model,” *MIS Quarterly* (27:1), pp. 51–90.

Google 2012. *Google Apps Marketplace*. http://www.google.com/enterprise/marketplace. Accessed 19 May 2012.

Gopal, A., and Gao, G. 2009. “Certification in the Indian Offshore IT Services Industry,” *Manufacturing & Service Operations Management* (11:3), pp. 471–492.

Hair, J. F., Hult, G. Tomas M., Ringle, C. M., and Sarstedt, M. 2013. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, Thousand Oaks, CA: Sage Publications.

Hu, X., Wu, G., Wu, Y., and Zhang, H. 2010. “The effects of Web assurance seals on consumers' initial trust in an online vendor: A functional perspective,” *Decision Support Systems* (48:2), pp. 407–418.

Hui, K.-L., Teo, H. H., and Lee, S.-Y. T. 2007. “The Value of Privacy Assurance: An Exploratory Field Experiment,” *MIS Quarterly* (31:1), pp. 19–33.

Kaplan, S. E., and Nieschwietz, R. J. 2003. “A Web assurance services model of trust for B2C e-commerce,” *International Journal of Accounting Information Systems* (4:2), pp. 95–114.

Khan, K. M., and Malluhi, Q. 2010. “Establishing Trust in Cloud Computing,” *IT Professional Magazine* (12:5), pp. 20–27.

Kim, D., and Benbasat, I. 2006. “The Effects of Trust-Assuring Arguments on Consumer Trust in Internet Stores: Application of Toulmin’s Model of Argumentation,” *Information Systems Research* (17:3), pp. 286–300.

Kim, D., and Benbasat, I. 2009. “Trust-Assuring Arguments in B2C E-commerce: Impact of Content, Source, and Price on Trust,” *Journal of Management Information Systems* (26:3), pp. 175–206.

Kim, K., and Kim, J. 2011. “Third-party Privacy Certification as an Online Advertising Strategy: An Investigation of the Factors Affecting the Relationship between Third-party Certification and Initial Trust,” *Journal of Interactive Marketing* (25:3), pp. 145–158.

Kimery, K. M., and McCord, M. 2006. “Signals of Trustworthiness in E-Commerce: Consumer

Understanding of Third-Party Assurance Seals," *Journal of Electronic Commerce in Organizations* (4:4), pp. 52–74.

Kirmani, A., and Rao, A. R. 2000. "No Pain, No Gain: A Critical Review of the Literature on Signaling Unobservable Product Quality," *Journal of Marketing* (64:2), pp. 66–79.

Lankton, N. K., and McKnight, D. H. 2011. "What Does it Mean to Trust Facebook? Examining Technology and Interpersonal Trust Beliefs," *ACM SIGMIS - Database for Advances in Information Systems* (42:2), pp. 32–54.

Lansing, J., Schneider, S., and Sunyaev, A. 2013. "Cloud Services Certifications: Measuring Consumers' Preferences for Assurances," in *Proceedings of the 21th European Conference on Information Systems,* Utrecht, Netherlands. 6-8 June, Paper 209.

Lee, J.-N., and Choi, B. 2011. "Effects of Initial and Ongoing Trust in IT Outsourcing: A Bilateral Perspective," *Information & Management* (48:2-3), pp. 96–105.

Lee, J.-N., Huynh, M. Q., and Hirschheim, R. 2008. "An Integrative Model of Trust on IT Outsourcing: Examining a Bilateral Perspective," *Information Systems Frontiers* (10:2), pp. 145–163.

Leimeister, S., Böhm, M., Riedl, C., and Krcmar, H. 2010. "The Business Perspective of Cloud Computing: Actors, Roles and Value Networks," in *Proceedings of the 18th European Conference on Information Systems*, T. Alexander, M. Turpin, and J. P. van Deventer (eds.), Pretoria, South Africa. June 7-9, Pretoria: University of Pretoria, Paper 56.

Li, X., Hess, T. J., and Valacich, J. S. 2008. "Why do we trust new technology? A study of initial trust formation with organizational information systems," *Journal of Strategic Information Systems, The* (17:1), pp. 39–71.

Li, X., Rong, G., and Thatcher, J. B. 2009. "Do We Trust the Technology? People? or Both? Ruminations on Technology Trust," in *Proceedings of the 15th Americas Conference on Information Systems (AMCIS 2009),* San Francisco, CA, USA. August 6 - 9, 2009.

Li, Y., and Chang, K.-c. 2012. "A Study on User Acceptance of Cloud Computing: A Multi-Theoretical Perspective," in *Proceedings of the 18th Americas Conference on Information Systems (AMCIS 2012),* Seattle, Washington, USA. August 9-11, 2012, Paper 19.

Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., and Wells, T. 2012. "Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers," *Journal of the American Society for Information Science and Technology* (63:4), pp. 755–776.

Mai, B., Menon, N. M., and Sarkar, S. 2010. "No Free Lunch: Price Premium for Privacy Seal-Bearing Vendors," *Journal of Management Information Systems* (27:2), pp. 189–212.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., and Ghalsasi, A. 2011. "Cloud Computing - The Business Perspective," *Decision Support Systems* (51:1), pp. 176–189.

Mauldin, E., and Arunachalam, V. 2002. "An Experimental Examination of Alternative Forms of Web Assurance for Business-to-Consumer e-Commerce," *Journal of Information Systems* (16:1), pp. 33–54.

Mayer, R., Davis, J., and Schoorman, F. 1995. "An Integrative Model of Organizational Trust," *Academy of Management Review* (20:3), pp. 709–734.

McKnight, D. H., Carter, M., Thatcher, J. B., and Clay, P. F. 2011. "Trust in a Specific Technology: An Investigation of Its Components and Measures," *ACM Transactions on Management Information Systems* (2:2), pp. 1–25.

McKnight, D. H., Choudhury, V., and Kacmar, C. 2002. "Developing and Validating Trust Measures for e-Commerce: An Integrative Typology," *Information Systems Research* (13:3), pp. 334–359.

McKnight, D. H., Cummings, L. L., and Chervany, N. L. 1998. "Initial Trust Formation in New Organizational Relationships," *Academy of Management Review* (23:3), pp. 473–490.

McKnight, D. H., Kacmar, C. J., and Choudhury, V. 2004. "Shifting Factors and the Ineffectiveness of Third Party Assurance Seals: A Two-Stage Model of Initial Trust in a Web Business," *Electronic Markets* (14:3), pp. 252–266.

Mell, P., and Grance, T. 2011. "The NIST Definition of Cloud Computing: NIST Special Publication 800-145," *Recommendations of the National Institute of Standards and Technology* 800-145, National Institute of Standards and Technology, Gaithersburg.

Narasimhan, B., and Nichols, R. 2011. "State of Cloud Applications and Platforms - The Cloud Adopters View," *Computer* (44:3), pp. 22–28.

Nöteberg, A., Christiaanse, E., and Wallage, P. 2003. "Consumer Trust in Electronic Channels," *e-Service Journal* (2:2), pp. 46–67.

Pavlou, P. A., Liang, H., and Xue, Y. 2007. “Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective,” *MIS Quarterly* (31:1), pp. 105–136.

Rao, A. R., and Bergen, M. E. 1992. “Price Premium Variations as a Consequence of Buyers' Lack of Information,” *Journal of Consumer Research* (19:3), pp. 412–423.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., and Camerer, C. 1998. “Not So Different After All - A Cross-Discipline View of Trust,” *Academy of Management Review* (23:3), pp. 393–404.

Sine, W. D., David, R. J., and Mitsuhashi, H. 2007. “From Plan to Plant: Effects of Certification on Operational Start-up in the Emergent Independent Power Sector,” *Organization Science* (18:4), pp. 578–594.

SoSci Survey 2013. *SoSci Panel for Scientists*. https://www.soscisurvey.de/panel/researchers.php. Accessed 28 April 2013.

Spence, M. 1973. “Job Market Signaling,” *The Quarterly Journal of Economics* (87:3), pp. 355–374.

Sunyaev, A., and Schneider, S. 2013. “Cloud Services Certification,” *Communications of the ACM* (56:2), pp. 33–36.

Vance, A., Elie-Dit-Cosaque, C., and Straub, D. W. 2008. “Examining Trust in Information Technology Artifacts: The Effects of System Quality and Culture,” *Journal of Management Information Systems* (24:4), pp. 73–100.

Venters, W., and Whitley, E. A. 2012. “A critical review of cloud computing: researching desires and realities,” *Journal of Information Technology* (27:3), pp. 179–197.

Wang, S., Beatty, S. E., and Foxx, W. 2004. “Signaling the trustworthiness of small online retailers,” *Journal of Interactive Marketing* (18:1), pp. 53–69.

Wang, W., and Benbasat, I. 2005. “Trust in and Adoption of Online Recommendation Agents,” *Journal of the Association for Information Systems* (6:3), pp. 72–101.

Zhang, H. 2005. “Trust Promoting Seals in Electronic Markets: Impact on Online Shopping Decisions,” *Journal of Information Technology Theory and Application (JITTA)* (6:4).

Zucker, L. G. 1986. “Production of Trust: Institutional Sources of Economic Structure, 1840–1920,” *Research in Organizational Behavior* (8), pp. 53–111.