EXPLAINING THE IMPACT OF CLOUD ASSURANCE SEALS ON CUSTOMERS' PERCEIVED PRIVACY

Research paper

Lang, Michael, Technical University of Munich, Munich, Germany, michael.lang@in.tum.de

Wiesche, Manuel, Technical University of Munich, Munich, Germany, wiesche@in.tum.de

Krcmar, Helmut, Technical University of Munich, Munich, Germany, krcmar@in.tum.de

Abstract

Privacy concerns inhabit professional cloud adoption. Assurance seals resulting from a third-party certification are frequently used from cloud service provider to provide privacy assurance for their customers. However, empirical findings on the effectiveness of assurance seals focusing on "who" issues those, even if customers also require the information why the assurance seal is valid and reliable. To fill this gap, we build on information integration theory and investigate the impact of certification authorities' reputation and the quality level of an audit on customers' perceived privacy within a professional cloud environment by using an experimental design including 43 professional cloud decision makers. We show that certification authorities' reputation does not alone produce opinion change, it rather affects customers' perceived privacy resulting from the quality level of an audit. Our findings have theoretical implications for the information integration theory and assurance seal research. We also discuss the managerial implications of our work for cloud service providers and certification authorities.

Keywords: Third-party certification; Assurance seal; Perceived privacy; Cloud computing; Information integration theory

1 Introduction

Privacy concerns remain a major inhabiting factor for the adoption of cloud services (Schneider and Sunyaev, 2016). To reduce privacy concerns, cloud service providers (CSPs) use audits to certify their products, processes or services through an independent authority and illustrate the results using assurance seals (Oezpolat et al., 2013, Lang et al., 2018b). Assurance seals decrease concerns of customers by providing the information as to which independent authority (e.g. certification authority) is providing assurance (e.g. privacy assurance) (Kimery and McCord, 2002, Lang et al., 2018a). As an example, the TÜV as a certification authority can certify according to the ISO 27001 standard that a CSP has a security management system that assures confidential, reliable, and secure treatment of customers' data and ordered services.

Research has frequently investigated the effectiveness of assurance seals. Several studies have identified a significant positive impact of assurance seals in terms of achieving their intended effects like reducing privacy concerns on digital services (Xu et al., 2012). Various other studies have been unable to confirm a significant impact of assurance seals in terms of achieving their intended effects like the improvement of location-based service selection behaviour (Keith et al., 2015) or the influence of consumers' perceived privacy risk (Xu et al., 2011). Hence, despite the popularity of assurance seals, research would benefit from a better understanding of what determines the effectiveness of assurance seals in an online environment (Oezpolat et al., 2013, Lowry et al., 2012).

Information integration theory explains why assurance seals' source and scope determine its effectiveness. The effectiveness of assurance seals describes the degree to which a certification achieves its intended effects (e.g. increasing perceived privacy) (Lins and Sunyaev, 2017). Information integration theory provides the framework for cognitive evaluation and the integration of information, e.g. from assurance seals (Sethi and King, 1999). Each item of information is determined by its weight (relative importance of an item of information) and scale value (semantic properties of an item of information) (Sethi and King, 1999, Lowry et al., 2008). While customers integrate assurance seals' source reputation to influence their overall perception (Lowry et al., 2008), the assurance seals' scope (e.g. privacy) must match the related concerns (e.g. privacy concerns) and determine the altitude (positive or negative) of an overall perception regarding an online service (Kim et al., 2015, Kimery and McCord, 2002). Therefore, research found two determinants – (1) third-parties' reputation and (2) the scope of an assurance seal – of the effectiveness of assurance seals.

To form privacy perceptions of customers regarding an online service effectively, customers also require, along with the source, information about the validity and reliability of the privacy assurance seals. Online services like cloud services are an ever-changing environment (Lins et al., 2016). Assurance seals' validity and reliability vary because of different levels of audit qualities (Oezpolat et al., 2013). While some assurance seals result from an in-depth or even continuous certification process, others only confirm that an online retailer has existed at the time of certification (Oezpolat et al., 2013). From trust-assuring arguments, we know they are most effective when customers receive reasons for why the argument is valid (Kim and Benbasat, 2006). As customers are able to differentiate between privacy assurance seals (Moores, 2005), we assume the validity and reliability of assurance seals determine their effectiveness to form privacy perceptions.

This paper addresses this gap and investigates how the source reputation and information about assurance seals' validity and reliability determines the effectiveness of privacy assurance seals. We build on the information integration theory (Anderson, 1981) and investigate the impact of certification authorities' reputation and the quality level of the audit process on customers' perceived privacy within a professional cloud environment. We show that certification authorities' reputation does not alone produce a change of opinion (Lowry et al., 2008), rather it affects customers' perceived privacy resulting from the quality level of the audit process.

To do this, we first outline the theoretical foundation of the information integration theory and develop the logic underlying the research hypotheses. Second, we present the research methodology and results.

The paper concludes with a discussion of the key findings, direction for future research, theoretical contribution and managerial implications of the results.

2 Theoretical background and hypotheses

2.1 Information integration theory

The information integration theory explains the cognitive integration of available information and addresses the question as to how people derive an overall attitudinal disposition from an array of knowledge and beliefs they hold about an attitude object (Anderson, 1981). For the cognitive integration of available information, two concepts are important: valuation and integration (Sethi and King, 1999).

Valuation refers to the process of determining the evaluative scale values and weights assigned to each item of information that contributes to attitudinal judgment. The weight parameter reflects the influence of the cognitive element in determining the overall attitude and can vary from zero to one with its value influenced by the context (Sethi and King, 1999). As an example, individuals weigh the importance of an item of information by the sources' reputation (Anderson, 1971). The scale value reflects semantic properties, varies from positive to negative and is considered independent of context and other cognitive elements (Sethi and King, 1999). As an example, the good or bad actions of presidents of the United States influenced their favorability and people's election behavior (Anderson, 1974).

Integration refers to the process of combining the information units into an overall attitudinal judgment. Individuals combine the weight and scale value parameters into a single judgment (Anderson, 1974). In this way, a weight parameter does not itself produce a change of opinion, but affects the degree of the stimulus resulting from the scale value of an item of information (Anderson, 1971).

The information integration theory is particularly useful in understanding the effects of assurance seals on information system customers. Simonin and Ruth (1998) demonstrate positive spill-over effects of highly reputable partners on lower reputable partners in a brand alliance. Lowry et al. (2008) extend such a finding by also demonstrating positive spill-over effects of brand seal from a highly reputable third-party on an unknown website. Both show how pre-existing impressions of an association with a known third-party combined with an unknown organization or website create an overall (positive or negative) impression (Lowry et al., 2008).

Assurance seals have different semantic properties and beside the weight parameter (e.g. certification authorities' reputation), the scale value is particularly important in determining the effectiveness of assurance seals. Kim and Benbasat (2006) identified that arguments consisting of the semantic properties as to what (assurance seals' scope) is assured and the reasons for why customers should rely on this information are most effective in influencing customers' perceptions. However, in contrast to Kim and Benbasat (2006), the source of the assurance seal is not the counterpart itself, instead the source is an independent third-party that is even more effective in influencing customers' perceptions (Kim and Benbasat, 2009). Therefore, in addition to the semantic properties, customers weigh the available information because of its personal relevance (Anderson, 1981).

To determine the CSPs' ability to protect privacy through assurance seals, customers integrate the available information about the certification authorities' reputation (source) and the quality level of an audit (validity and reliability) (similar to "weights" and "scale value" in information integration theory) into their information processing to form an overall perception about the CSP (Anderson, 1981, Simonin and Ruth, 1998). Certification authorities' reputation influences the personal relevance of the information (Lowry et al., 2008, Anderson, 1971). In line with Anderson (1974), the quality level of an audit determines the scale value to protect privacy. To understand how different degrees of the effectiveness of assurance seals occur, it is important to consider both dimensions (weight and scale value).

2.2 Customers' privacy perceptions and assurance seals in a cloud environment

2.2.1 Perceived privacy in an online environment

In an online environment, a perceived state of privacy (short perceived privacy) refers to an aggregation of consumers' perceptions and expectations regarding a provider's characteristics when storing or processing sensitive information (Chellappa, 2008, Frye and Dornisch, 2010). A group of scholars (Bansal et al., 2015, Smith et al., 1996) includes customers' perceptions regarding collection and subsequent access, use, and disclosure of sensitive information as representative characteristics that influence one's privacy perceptions. Collection refers to what sensitive information a provider collects from a customer. Access refers to whether or not reasonable steps are in place to assure that sensitive information is accurate and secure from unauthorized use. Use refers to whether or not sensitive information will be used for purposes other than those for which they have been provided. Disclose refers to whether or not sensitive information is disclosed to secondary parties. Perceived privacy results when consumers compare the actual and expected collection and subsequent access, use, and disclosure of their sensitive information (Chellappa, 2008, Frye and Dornisch, 2010).

Therefore, perceived privacy reflects the amount of consumers' belief that the institutional setup allows for the privacy of their transaction to be maintained as promised. Perceived privacy is defined as "an individual's self-assessed state in which external agents have limited access to information" (Smith et al., 2011).

2.2.2 Privacy assurance seals in a cloud environment

Cloud computing "is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" (Mell and Grance, 2011). Customers use these resources to process, transfer, and store sensitive information, such as personal data from their customers, and to gain advantages with respect to costs and flexibility (Mell and Grance, 2011, Böhm et al., 2010). However, existing information asymmetry between the customer and the CSP and resulting privacy concerns serve as major inhibitors in adopting cloud services.

To overcome privacy concerns, customers seek an independent third-party certification and resulting assurance seals to assure privacy when adopting cloud services (Yang and Tate, 2012, Lang et al., 2017, Lang et al., 2016). Privacy assurance seals inform (potential) customers of a CSP in three dimensions (Lansing et al., 2018): First, whether the provider complies with the certification scope. Second, information about the certification process itself. Third, the issuers brand of the assurance seal.

To obtain an assurance seal, a CSP typically goes through a certification process administered by a certification authority. Such certification processes include an audit to verify the quality specification from the certification scope, for instance, contractual requirements (e.g. service level agreements), legal requirements (e.g. privacy policy), security requirements (e.g. encryption), business processes (e.g. data protection management), and data center infrastructure (e.g. physical access control) (Sunyaev and Schneider, 2013). Depending on the audit process, static versus continuous, an audit takes place typically every third year or continuously, respectively (Anisetti et al., 2017, Lins et al., 2016). Upon successful completion of this process, the CSP is permitted to display the assurance seal and an attestation report on its website.

Figure 1 summarizes the involved roles and interactions to obtain an assurance seal from the certification authority.

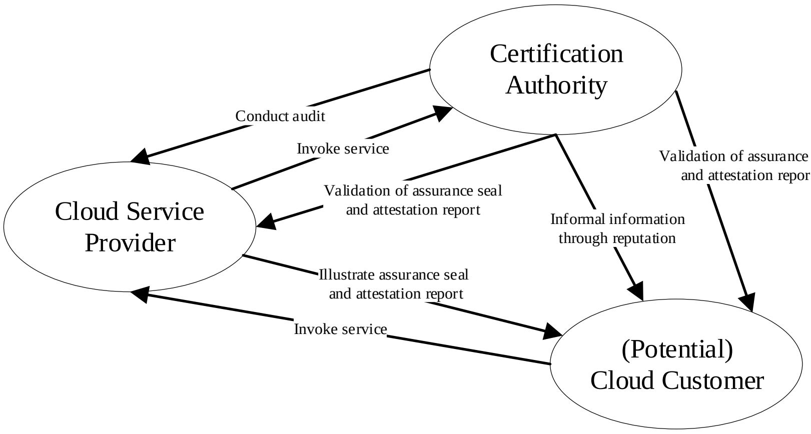
Certification Authority
Cloud Service Provider
(Potential) Cloud Customer
Conduct audit
Invoke service
Validation of assurance seal and attestation report
Informal information through reputation
Validation of assurance seal and attestation report
Illustrate assurance seal and attestation report
Invoke service

Figure 1. Involved roles and interactions to obtain an assurance seal

2.2.3 Source of an assurance seal

In a professional service engagement, e.g. cloud service certification, customers do not enjoy perfect information to determine a service quality (Shaked and Sutton, 1982). As a result of imperfect information, customers frequently rely on companies' reputation as a surrogate measure of quality (Barzel, 1982). As it is expensive and takes a long period of time for certification authorities to build a high reputation, certification authorities avoid verification or attestation services that do not meet the communicated privacy requirements (Zhao et al., 2009, Tang et al., 2008, Yamagishi and Yamagishi, 1994). Reputational losses would be fatal for certification authorities due to the high degree of competition in the certification market (Zhao et al., 2009). When source reputation is high, the information presented by the source is perceived to be useful (Ko et al., 2005). Customers integrate the available information from reputable certification authorities with information about the CSP to generate their overall perceptions (Anderson, 1981). Customers use the source of the assurance seals to apply weights and prefer those issued by highly reputable third parties (Kimery and McCord, 2002, Lala et al., 2002, Lowry et al., 2008). Customers also associate positive perception regarding the third-party with the lesser-known or even unknown CSPs (Lowry et al., 2008, Simonin and Ruth, 1998). A certification authority's high reputation increases the perceived effect of the communicated audit for the protection of customers' privacy and positively influences the perceived privacy in a professional cloud environment:

> ***Hypothesis 1 (H1):*** *Customers' perceived privacy of cloud service providers is a positive function of the certification authorities' reputation as the quality level of an audit remains constant.*

2.2.4 Quality level of an assurance seal audit

The certification authorities provide assertions through audits about the ability and the state of the CSP to secure and protect data (Oezpolat et al., 2013). While some assurance seals are based on a high quality level of an audit including an in depth certification process, e.g. the ISO 27001, TRUSTe, WEBTRUST or CyberTrust seal, others are based on a low quality level of an audit that only publishes a directory of trusted online retailers, e.g. BBB On-Line (Oezpolat et al., 2013). With more effort made in verifying the security of the CSP, the certification authorities improve their security and privacy knowledge and technologies (Anderson and Moore, 2006). With the increasing quality level of an audit, the ability to observe a privacy breach increases (Lee et al., 2013). Based on this information, customers understand why assurance seals in place are valid and reliable in effectively protecting their privacy (Kim and Benbasat, 2006). When the quality level of an audit is high, customers value the information more in comparison to if the quality level of an audit is low (Kim and Benbasat, 2006). This holds particularly true in an ever-changing cloud environment where customers doubt the validity and reliability of audits with a low quality level (Lins et al., 2016, Anisetti et al., 2017). Similar to our previous argumentation, customers integrate the information about the quality level of an audit conducted by a certification authority with the information about privacy protection activities of the CSP to generate their overall perceptions (Anderson, 1981). A high quality level of an audit signals successful protection of customers' privacy and, therefore, positively influences the perceived privacy in a professional cloud environment:

> ***Hypothesis 2 (H2):*** *Customers' perceived privacy of cloud service providers is a positive function of the quality level of an audit as the certification authorities' reputation remains constant.*

2.3 Effective form of assurance seals

Customers integrate information about the reputation of a certification authority and its quality level of an audit to form their overall perception. Customers value information like the quality level of an audit to understand why an item of information is valid and reliable (Kim and Benbasat, 2006). Moreover, depending on the source of information, information differs in terms of the relevance to the customer (Lowry et al., 2008). The certification authority's reputation does not itself produce a change of opinion, but affects the degree of the stimulus resulting from the quality level of an audit (Anderson, 1971). Similar to our previous argumentation, customers integrate these pieces of information with the information about the cloud service to generate their overall perceptions (Anderson, 1981). A highly reputable certification authority that conducts a high quality level of an audit outperforms a low (highly) reputable certification authority that conducts a high (low) quality level of an audit in terms of perceived privacy in a professional cloud environment:

> ***Hypothesis 3 (H3):*** *Customers' perceived privacy of cloud service providers is higher for highly reputable certification authorities that conduct a high quality level of an audit than for a low (highly) reputable certification authority that conducts a high (low) quality level of an audit.*

Our research model is illustrated in Figure 2.

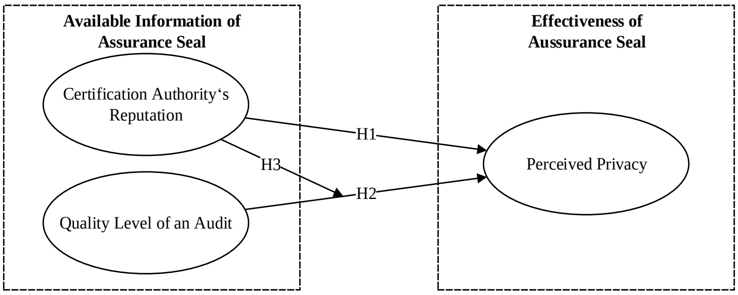
Available Information of Assurance Seal
Certification Authority's Reputation
Quality Level of an Audit
H1
H2
H3
Effectiveness of Aussurance Seal
Perceived Privacy

Figure 2. Proposed research model to investigate the effectiveness of assurance seals

3 Research method

3.1 Research design

We used an experimental design because it allows for the manipulation of variables and the testing of causal relationships. We used a within-subject experimental design to control for subject variability (it accounts for individual differences when subjects serve as their own control) (Keppel, 1991). In addition, a within-subject design provides us the opportunity to simulate repeated decisions, a frequently occurrence in real life (Andriole, 2007). Specifically, we employed a 2 (high/ low certification authorities' reputation) X 2 (high/ low quality level of an audit) within-subject factorial design. We also employed a baseline scenario without any manipulation (see Figure 3).

3.2 Experimental manipulations

The reputation of certification authorities and the quality level of an audit were operationalized using an online-based free simulation experiment combined with the scenario-based method. Whereas standard laboratory experiments rely on a treatment to vary one or more independent variables, free simulation experiments expose the subjects to a number of realistic tasks – for example, by identifying an appropriate CSP. A core feature of free simulation experiments is the interaction of subjects with a simulated website; this feature is frequently used in online studies to increase realism and generalizability (Gefen et al., 2003, Burton-Jones and Straub, 2006, Lowry et al., 2012). Website conditions ranged freely and widely as subjects interacted naturally although all subjects received treatment materials. The realistic task and the natural interaction allow subjects to form meaningful perceptions before answering related questions (Gefen et al., 2003, Söllner et al., 2015).

Scenarios illustrate possible states of a cloud service. Scenarios provide a form or tool to study a possible and plausible state, and to create awareness of which applications are possible (Bria et al., 2001). Free-simulated online experiments, including different scenarios, are frequently used in experimental studies to manipulate different conditions of variables, simulate customers tasks or represent context for study (Lowry et al., 2012, Xu et al., 2012). We used five scenarios in a free-simulated online experiment to investigate which information determine the effectiveness of assurance seals to protect privacy.

		Certification authorities’ reputation	
		low	high
Quality level of an audit	low	(1)	(2)
	high	(3)	(4)

A baseline scenario with no manipulation was also simulated (5)

Figure 3. Research design

We manipulated the certification authorities’ reputation and the quality level of an audit using four variant scenarios. We added a baseline scenario in which no manipulation occurred. To vary certification authorities’ reputation, we used certification authorities with high (e.g., TÜV – international well-known certification authority) versus low (e.g., CERTIFYER[1] – newly developed certification authority[2]) reputation.

To vary the quality level of an audit, we used different attestation processes and related attestation timings: an attestation through a static certification (e.g., attestation took place 2 years ago) and a continuous certification which was continuously updated (e.g., attestation took place 1 week ago). Since continuous certification involves “high efforts for agent development and implementation” (Lins et al., 2016) for the audit and high effort for the continuous verification and attestation process, the quality level of an audit for a continuous certification is higher than for the a static certification.

Overall, a total of four manipulated scenarios and one baseline scenario were presented to subjects: (1) low certification authorities’ reputation and low quality level of an audit; (2) high certification authorities’ reputation and low quality level of an audit; (3) low certification authorities’ reputation and high quality level of an audit; (4) high certification authorities’ reputation and high quality level of an audit. To assure comparable results, we used ISO 27001 as a well-known certification scope for all four scenarios. The last scenario was a baseline scenario in which no manipulation occurred (5).

Two variables, certification authorities’ reputation and quality level of an audit, were manipulated in the experiment. The manipulation was illustrated within two different levels of detail. First, each manipulation was on the scenarios’ main page as an assurance seal, identification of certification authority, certification scope and identification of attestation process. Second, each manipulation was accessible within the certification attestation report. As an example, Figure 4 illustrates scenario (3) including the possible navigations to the certification attestation report.

[1] The name of the newly developed certification service was blinded for confidential reasons.

[2] Lowry et al. (2008) provide empirical evidence that the reputation of unknown third-parties is significantly lower than the reputation of a known and highly reputable organization.

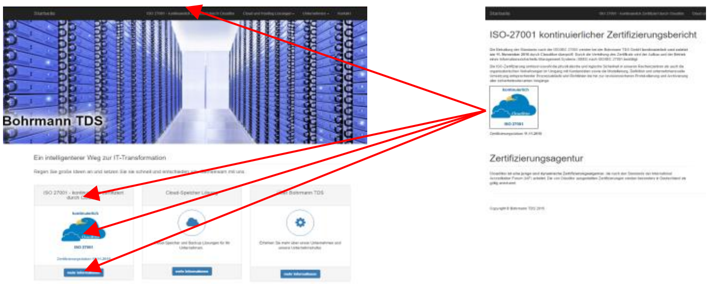
Startseite
Bohrmann TDS
Ein intelligenterer Weg zur IT-Transformation
ISO 27001 - kontinuierlich zertifiziert durch Cloud...
Cloud-Speicher Lösungen
Über Bohrmann TDS
kontinuierlich
ISO 27001
mehr Informationen
ISO-27001 kontinuierlicher Zertifizierungsbericht
Zertifizierungsagentur

Figure 4. The main page of scenario (3) (left) including possible navigation paths (red arrows) to certification attestation report (right)

Each certification attestation report consists of three major parts. First, the certification process was described including the last attestation date. Second, background information (size and acting regions) on the certification authority was provided. Third, some background information about the ISO 27001 certification was provided; this information was not changed across all manipulations, ensuring a common understanding regarding the assurance seal and attestation report that is in place (Lowry et al., 2012).

3.3 Measurement

The measurement of formative constructs is highly dependent on the related domain (Petter et al., 2007). To provide comparable results for privacy across different domains, we used a reflective construct (Siponen and Vance, 2014). For our dependent variable, we used the three reflective measurements of perceived privacy from Dinev et al. (2013) and adapted the wording to a professional cloud environment (see Table 1).

Constructs and items (measured on a seven-point, Likert-type scale)		**Source**
Perceived privacy	I feel I have enough data privacy when I use this cloud service provider.	Dinev et al. (2013)
	I am comfortable with the amount of data privacy with this cloud service provider.	
	I think data privacy is preserved when I use this cloud service provider.	
Manipulation check – reputation	In this scenario, the certification authority has a high reputation in the market.	Self-developed
Manipulation check – quality level of an audit	In this scenario, the certification process was based on a continuous certification process. (measured on a yes/no scale)	Self-developed

Table 1. Measurement items and manipulation checks

Since not all subjects were fluent in English, the experiment as well as the questionnaire were provided in German. To check for translation bias within the measurement items, a back-translation technique was employed in which two different translators translated the German questionnaire back into English (Bhattacherjee and Park, 2014). The back-translated items had a high degree of correspondence with the original English items (see Table 1) assuring the relative lack of translation bias.

3.4 Research procedures

Approximately two months before initiating the experiment each subject received an e-mail with a personalized pre-experiment survey link inviting them to sign up for the experiment. During this phase, we received their consent to participate, and we collected the pre-experiment measures to reduce the risk of common methods bias (Podsakoff et al., 2003). The pre-experimental measures included cloud computing experience, and familiarity with ISO 27001 certification. The latter was important to assure each subject understood the meaning and sense of the ISO 27001 assurance seal (Lowry et al., 2012). Because we collected this information prior to the experiment, the experimental site did not influence these measures. Figure 5 illustrates the entire research process.

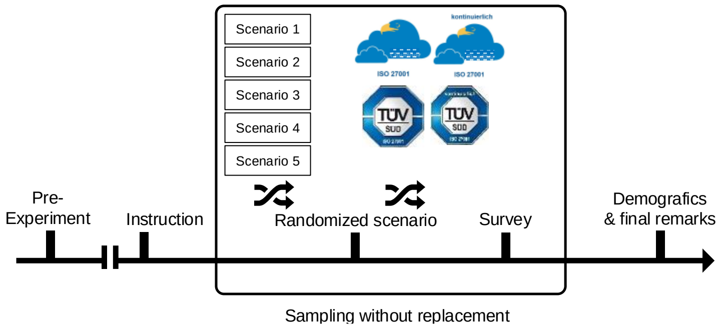

Figure 5. Research procedures

During the experiment, all subjects received and read the same instructions. Subjects were asked to identify an appropriate CSP that offers cloud storage for their data. Subsequently, each subject was presented with five scenarios of CSP websites in which – except for the baseline condition – different certification authorities' reputation (high versus low) were offered with different quality levels of an audit (high versus low). The presentation of each scenario was followed by a survey. This included manipulation check questions and questions that measured the subject's perceived privacy based on the presented scenario (see Table 1). Each subject was asked to answer the questionnaire in regard to the experienced scenario. The last part of the experiment captured subjects' demographic information (e.g., age and gender) and final remarks.

To minimize possible learning and ordering effects of scenarios on subjects, we considered three strategies. First, we presented the scenarios in a randomized order. Second, subjects were asked, after each scenario and at the end of the experiment, an open question asking which information they used as a basis for their judgments and if any irregularities occurred. Last, we tracked each subject's duration time to navigate through our experimental websites. The average duration time of subjects within each scenario was 3.8 minutes; subjects navigated through our experimental websites, including the attestation report, without any obvious patterns. No evidence of learning or ordering effects were observed.

We carried out a pilot study with research fellows to evaluate the clarity of the scenarios and the items in the questionnaire. No major issues were identified during the pilot study; the pilot subjects made minor suggestions on wording and phrasing that were incorporated into the questionnaire and experimental websites. After another review round, we conducted the experiment.

3.5 Subjects

We adopted a purposive sampling technique. This is a non-probability sampling that conforms to certain criteria (Cooper and Emory, 1995). Previous studies have suggested that certificates are only effective when subjects understand their meaning and sense (Lowry et al., 2012). To confirm these preconditions, we focused on professional cloud decision makers. Therefore, our reason for choosing purposive sampling is that professional cloud decision makers are rare and only selected subjects are suitable for our study.

Subjects were recruited from medium- and large-sized German companies across different industries. 71 suitable subjects were identified and contacted. Finally, a total number of 43 subjects participated in this study. All subjects were native German speakers. Demographic information and the cloud experience of the subjects is presented in Table 2.

The subjects recruited in this study had extensive cloud experience and were familiar with the certificate ISO 27001 (see Table 2). All subjects' job descriptions were related to selecting and purchasing cloud-services. This ensures reliable results based on experienced professionals within a cloud environment (Siponen and Vance, 2014).

Demographics		Frequency	Percent	Experience		Frequency	Percent
Age	<31	6	14	Professional cloud experience	<2 years	10	23
	31-40	9	22		3-5 years	15	35
	41-50	14	32		6-8 years	11	25
	>50	14	32		>8 years	3	7
Sex	Female	3	7	Certificate familiarity	yes	43	100
	Male	40	93		no	0	0

Table 2. Demographic and experience information of subjects

Assuming a medium effect size (f = 0.25), with a power of 0.80 at alpha equals 0.05 significance level, the required sample size for each cell is 39 (Cohen, 1992). Hence, 43 subjects for each experimental treatment is adequate for data analysis.

3.6 Manipulation checks

The manipulation of certification authorities' reputation and the quality level of an audit was assessed following the presentation of each scenario (see Table 1 for the manipulation check questions). These questions were used to test the subjects' interpretation and understanding of the scenarios.

We conducted paired-sample T-tests to test the effectiveness of the manipulations. The results show that all treatments were manipulated effectively. First, subjects perceived scenarios in which TÜV served as a certification authority to have a higher reputation than those scenarios with the low certification authorities' reputation CERTIFYER (mean difference = 2.69, std. deviation = 0.44, t = 6.05, $p < 0.05$). Second, subjects perceived that those scenarios with a continuous certification provided greater perception regarding the continuous and up-to-date attestation of third-party certification than the static certification scenarios (mean difference = 0.79, std. deviation = 0.24, t = 3.22, $p < 0.05$).

3.7 Factor analysis

The reflective construct perceived privacy is validated using the standard procedure documented by Straub (1989). All factor loadings are significant suggesting convergent validity. Perceived privacy satisfies the threshold values for the average variance extracted (AVE > 0.50) and Cronbach's alpha (alpha > 0.70) as suggested by Straub (1989). To evaluate construct reliability, we calculated composite reliability (CR) for perceived privacy. Perceived privacy has a composite reliability significantly above the cut-off value of 0.70. In sum, perceived privacy's quality is satisfactory.

4 Results

4.1 Testing the research model

Data associated with perceived privacy was analyzed using a repeated-measure ANOVA test with two within-subject factors as independent variables: certification authorities' reputation and the quality level of an audit. The mean values and standard deviations are reported in Table 3.

Within-subject factors		Perceived privacy	
Certification authorities' reputation	**Quality level of an audit**	**Mean**	**Standard deviation**
Baseline (no treatment)	Baseline (no treatment)	3.124	0.229
Low reputable certification authority	Static certification	3.419	0.254
	Continuous certification	4.101	0.267
High reputable certification authority	Static certification	3.829	0.218
	Continuous certification	4.512	0.255

Table 3. Means and standard deviations for perceived privacy

To test Hypotheses 1, a contrast test was conducted based on the Wilks-Lambda test (Kirk, 1982). H1: *Customers' perceived privacy of cloud service providers is a positive function of the certification authorities' reputation as the quality level of an audit remains constant*, is supported. Table 4 reports for the manipulation contrast test for perceived privacy a contrast value = 0.746, F-Value = 14.274 and p-Value < 0.001.

To test Hypotheses 2, a contrast test was conducted based on the Wilks-Lambda test (Kirk, 1982). H2: *Customers' perceived privacy of cloud service providers is a positive function of the quality level of an audit as the certification authorities' reputation remains constant*, is also supported. Table 4 reports for the manipulation contrast test for perceived privacy a contrast value = 0.908, F-Value = 4.236 and p-Value < 0.05.

Hypothesis	**Contrast value**	**F-Value**	**p-Value**	**Hypothesis supported?**
H1	0.746	14.274	<0.001	Yes
H2	0.908	4.236	0.023	Yes

Table 4. Manipulation contrast tests for perceived privacy

To test Hypotheses 3, two further contrast tests were conducted based on the Wilks-Lambda test (Kirk, 1982). H3: *Customers' perceived privacy of cloud service providers is higher for highly reputable certification authorities that conduct a high quality level of an audit than for a low (highly) reputable certification authority that conducts a high (low) quality level of an audit*, is supported. In this analysis, we first (a) compared certification authorities of high reputation and high quality level of an audit with certification authorities of high reputation and low quality level of an audit. Table 5 reports for the manipulation contrast test for perceived privacy a contrast value = 0.804, F-Value = 10.223 and p-Value < 0.05. We second (b) compared certification authorities of high reputation and high quality level of an audit with certification authorities of low reputation and high quality level of an audit. Table 5 reports for the manipulation contrast test for perceived privacy a contrast value = 0.927, F-Value = 3.299 and p-Value < 0.1.

Hypothesis	**Contrast test between certification authorities**	**Contrast value**	**F-Value**	**p-Value**	**Hypothesis supported?**
H3	(a) high reputation and low quality level of an audit against high reputation and high quality level of an audit	0.804	10.223	0.001	Yes
	(b) low reputation and high quality level of an audit against high reputation and high quality level of an audit	0.927	3.299	0.038	

Table 5. Additional manipulation contrast tests for perceived privacy

4.2 Additional analysis

To test if any assurance seal influences customers' perceived privacy, four baseline contrast tests were conducted based on the Wilks-Lambda test (Kirk, 1982). Certification authorities of high reputation and low quality level of an audit (contrast value = 0.615, F-Value = 26.248, p-Value < 0.001), low reputation and high quality level of an audit (contrast value = 0.750, F-Value = 14.032, p-Value < 0.001) and high reputation and high quality level of an audit (contrast value = 0.421, F-Value = 55.503, p-Value < 0.001), perceived privacy was significantly higher than of the perceive privacy rating of the baseline scenario. Perceived privacy resulting from low certification authorities' reputation and low quality level of an audit was higher on a marginally significant level (contrast value = 0.926, F-Value = 3.371, p-Value < 0.05) than the baseline scenario as well (see *Table 6*). Therefore, within our experiment any assurance seal can increase customers' perceived privacy in a professional cloud environment.

Baseline contrast test against certification authorities of:	Contrast value	F-Value	p-Value
… low reputation and low quality level of an audit	0.926	3.371	0.036
… high reputation and low quality level of an audit	0.615	26.248	<0.001
… low reputation and high quality level of an audit	0.750	14.032	<0.001
… high reputation and high quality level of an audit	0.431	55.503	<0.001

Table 6. Baseline contrast tests for perceived privacy

5 Discussion

5.1 Findings

Our research demonstrates that a customers' perceived privacy in a professional cloud environment can be increased by the provisioning of relevant information through assurance seals provided by an independent certification authority. Therefore, the customers' perceptions and beliefs regarding the assurance seal are not replaced by new information of the unknown CSP, rather old perceptions and beliefs of the source, and semantic properties of an assurance seal are integrated with the information to form new attitudes regarding the unknown CSP.

Our findings suggest that certification authorities' reputation and the quality level of an audit are important information to shape customers' perceptions, including perceived privacy and, in doing so, determine the effectiveness of assurance seals in a professional cloud environment. When the certification authorities' reputation and the quality level of an audit are high, the highest effects of assurance seals on customers' perceived privacy are identified during CSP selection.

5.2 Study contribution and theoretical and managerial implications

Our findings extend research by explaining how semantic properties of assurance seals are integrated to form customers' perceptions. Customers are not only able to differentiate between high and low levels of source reputation, also about high and low levels of semantic properties of assurance seals. In particular, information in regard to the reliability and validity of an assurance seal are important semantic properties that contributes to the attitudinal judgment. Consistent with the information integration theory (Anderson, 1981), third-parties' reputation does not alone produce opinion change and determine assurance seals effectiveness (Lowry et al., 2008), it rather influences the effect size of the opinion change on how and what interaction the third-party has.

Our findings extend research by considering semantic properties of assurance seals. To protect privacy in a professional cloud environment, customers not only consider "who" provides which assurance seal, they also consider "how" the assurance seal is reached. Hence, as customers face information asymmetry and cannot assure privacy by themselves, semantic properties are important to evaluate the validity and reliability of an assurance seal. Therefore, when investigating the effectiveness of assurance seals in online environments the information who protect what and how should be considered and communicated.

However, we notice that perceived privacy resulting from low certification authorities' reputation and low quality level of an audit was higher on a marginally significant level than the baseline scenario having no assurance seal. Such findings are in line with the inconsistent findings in literature (Oezpolat et al., 2013). Therefore, we conclude, research should be careful in selecting assurance seals of low reputable certification authorities or low quality level of an audit when investigating assurance seals.

From a practitioner point of view, our results suggest that CSPs can influence perceptions of their customers by implementing assurance seals. Hence, CSPs should consider certification authorities to prove their data protection capabilities. However, not all assurance seals influence the perception of customers in the same manner. CSPs should particular choose assurance seals with a high quality level of an audit like continuous certificates issued from a high reputable certification authority.

Our results also provide conclusion for certification authorities. To be effective, any certification authority need to use a certain strategy to communicate their reputation and quality level of an audit. Our study shows that the usage of certificates combined with an attestation report is one effective example for such a communication strategy. An assurance seal including the certification scope, certification method and certification authority in combination with a certification attestation report is effective in creating a retrieval cue for customers' privacy perception.

5.3 Limitations and future research

All research is subject to limitations. Here, one possible limitation of our work relates to the method used to operationalize high and low certification authorities' reputation and quality level of an audit. We used scenarios to manipulate the different conditions of high and low certification authorities' reputation and quality level of an audit. Scenarios were presented to the subjects before capturing their perceived privacy. One may argue that a real CSP website will provide a more realistic experience to subjects and produces more reliable and meaningful results. However, considering that continuous certification to provide high quality level of an audit is still very new and not readily available, the scenario-based approach allows us to study this emerging phenomenon without the constraints of time and state-of-the-art technology.

This study was conducted in Germany. Therefore, care must be taken when attempting to generalize the privacy results to other social, economic, legal and cultural environments. Privacy is a relative concept and may be related to cultural values (Kim et al., 2015) – what is considered private in one culture or legal region may not be considered private in another culture or legal region. For example, people in the United States tend to take the perspectives of "privacy pragmatists" while Europeans (including Germans) are concerned about their privacy and are more likely to take the perspectives of "privacy fundamentalists" (Galanxhi and Nah, 2006).

Last, our limited number of subjects were recruited using a purposive selection approach. While our professionals were all familiar with assurance seals, future research can take this investigation further by drawing research subjects from a more diverse, randomly selected, and comprehensive population.

6 Conclusion

This research investigates the influence of assurance seals on customers' perceived privacy within a professional cloud environment. By focusing on the two information dimensions certification authorities' reputation and the quality level of an audit, this research has important theoretical and managerial implications. Results of this study are important in situations when customers face information asymmetry and cannot assure privacy by themselves.

From a theoretical point of view, our research extends the information integration theory by demonstrating how source reputation affects customers' perceived privacy resulting from information how a third-party and an unknown CSP interact. Second, we provide an empirical evidence about the effectiveness of assurance seals within a professional cloud environment. Third, this research provides two information dimensions, namely certification authorities' reputation and the quality level of an audit, which interact and determine the effectiveness of assurance seals in a cloud environment. From a managerial point of view, we contribute to CSPs and certification authorities.

Acknowledgement

This research was funded by the German Federal Ministry for Education and Research (grant. No. 16KIS0078).

References

Anderson, N. H. (1971). "Integration theory and attitude change." *Psychological Review* 78 (3)**,** 171-206.

Anderson, N. H. (1974). "Cognitive algebra: Integration theory applied to social attribution." *Advances in Experimental Social Psychology* 7**,** 1-101.

Anderson, N. H. (1981). *Foundations of information integration theory.* New York: Academic Press.

Anderson, R. and T. Moore (2006). "The economics of information security." *Science* 314 (5799)**,** 610-613.

Andriole, S. J. (2007). "Mining for digital gold: technology due diligence for CIOs." *Communications of the Association for Information Systems* 20 (1)**,** 371-381.

Anisetti, M., C. Ardagna, E. Damiani, N. El Ioini and F. Gaudenzi (2017). "Modeling time, probability, and configuration constraints for continuous cloud service certification." *Computers & Security* 72**,** 234-254.

Bansal, G., F. Zahedi and D. Gefen (2015). "The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern." *European Journal of Information Systems* 24 (2015)**,** 624-644.

Barzel, Y. (1982). "Measurement cost and the organization of markets." *Journal of Law & Economics* 25 (1)**,** 27-48.

Bhattacherjee, A. and S. C. Park (2014). "Why end-users move to the cloud: a migration-theoretic analysis." *European Journal of Information Systems* 23 (3)**,** 357-372.

Böhm, M., G. Koleva, S. Leimeister, C. Riedl and H. Krcmar (2010). Towards a generic value network for cloud computing. *International Workshop on Grid Economics and Business Models.* Berlin Heidelberg: Springer.

Bria, A., F. Gessler, O. Queseth, R. Stridh, M. Unbehaun, J. Wu, J. Zander and M. Flament (2001). "4th-generation wireless infrastructures: scenarios and research challenges." *IEEE Personal Communications* 8 (6)**,** 25-31.

Burton-Jones, A. and D. W. Straub (2006). "Reconceptualizing system usage: An approach and empirical test." *Information Systems Research* 17 (3)**,** 228-246.

Chellappa, R. K. (2008). Consumers' trust in electronic commerce transactions: the role of perceived privacy and perceived security. Emory University, Atlanta, GA.

Cohen, J. (1992). "A power primer." *Psychological Bulletin* 112 (1)**,** 155-159.

Cooper, D. R. and C. W. Emory (1995). *Business Research Methods.* Chicago: IRWIN.

Dinev, T., H. Xu, J. H. Smith and P. Hart (2013). "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts." *European Journal of Information Systems* 22 (3)**,** 295-316.

Frye, N. E. and M. M. Dornisch (2010). "When is trust not enough? The role of perceived privacy of communication tools in comfort with self-disclosure." *Computers in Human Behavior* 26 (5)**,** 1120-1127.

Galanxhi, H. and F. F. H. Nah (2006). "Privacy issues in the era of ubiquitous commerce." *Electronic Markets* 16 (3)**,** 222-232.

Gefen, D., E. Karahanna and D. W. Straub (2003). "Inexperience and experience with online stores: The importance of TAM and trust." *IEEE Transactions on Engineering Management* 50 (3)**,** 307-321.

Keith, M. J., J. S. Babb, P. B. Lowry, C. P. Furner and A. Abdullat (2015). "The role of mobile-computing self-efficacy in consumer information disclosure." *Information Systems Journal* 25 (6)**,** 637-667.

Keppel, G. (1991). *Design and analysis: A researcher's handbook.* Englewood Cliffs: Prentice-Hall, Inc.

Kim, D. and I. Benbasat (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)**,** 286-300.

Kim, D. and I. Benbasat (2009). "Trust-assuring arguments in B2C e-commerce: Impact of content, source, and price on trust." *Journal of Management Information Systems* 26 (3)**,** 175-206.

Kim, D. J., M.-S. Yim, V. Sugumaran and H. R. Rao (2015). "Web assurance seal services, trust and consumers' concerns: An investigation of e-commerce transaction intentions across two nations." *European Journal of Information Systems* 25 (3)**,** 252-273.

Kimery, K. M. and M. McCord (2002). "Third-party assurances: Mapping the road to trust in e-retailing." *Journal of Information Technology Theory and Application* 4 (2)**,** 63-82.

Kirk, R. E. (1982). *Experimental design.* Published Online: John Wiley & Sons, Inc.

Ko, D.-G., L. J. Kirsch and W. R. King (2005). "Antecedents of knowledge transfer from consultants to clients in enterprise system implementations." *Management Information Systems Quarterly* 29 (1)**,** 59-85.

Lala, V., V. Arnold, S. G. Sutton and L. Guan (2002). "The impact of relative information quality of e-commerce assurance seals on Internet purchasing behavior." *International Journal of Accounting Information Systems* 3 (4)**,** 237-253.

Lang, M., M. Wiesche and H. Krcmar (2016). What are the most important criteria for cloud service provider selection? A Delphi study. *European Conference on Information Systems.* Istanbul.

Lang, M., M. Wiesche and H. Krcmar (2017). Conceptualization of Relational Assurance Mechanisms - A Literature Review on Relational Assurance Mechanisms, Their Antecedents and Effects. *International Conference on Wirtschaftsinformatik.* St. Gallen.

Lang, M., M. Wiesche and H. Krcmar (2018a). "Criteria for Selecting Cloud Service Providers: A Delphi Study of Quality-of-Service Attributes." *Information & Management*.

Lang, M., M. Wiesche and H. Krcmar. "Perceived Control and Privacy in a Professional Cloud Environment." Hawaii International Conference on System Sciences. 2018b Big Island, Hawaii. p.

Lansing, J., A. Sunyaev and A. Benlian (2018). "'Unblackboxing Decision Makers' Interpretations of IS Certifications in the Context of Cloud Service Certifications." *Journal of the Association for Information Systems* forthcoming.

Lee, C. H., X. Geng and S. Raghunathan (2013). "Contracting information security in the presence of double moral hazard." *Information Systems Research* 24 (2)**,** 295-311.

Lins, S., S. Schneider and A. Sunyaev (2016). "Trust is good, control is better: Creating secure clouds by continuous auditing." *IEEE Transactions on Cloud Computing* PP (99).

Lins, S. and A. Sunyaev. "Unblackboxing IT Certifications: A Theoretical Model Explaining IT Certification Effectiveness." International Conference on Information Systems. 2017 Soul. p.

Lowry, P. B., G. Moody, A. Vance, M. Jensen, J. Jenkins and T. Wells (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)**,** 755-776.

Lowry, P. B., A. Vance, G. Moody, B. Beckman and A. Read (2008). "Explaining and predicting the impact of branding alliances and web site quality on initial consumer trust of e-commerce web sites." *Journal of Management Information Systems* 24 (4)**,** 199-224.

Mell, P. and T. Grance (2011). The NIST definition of cloud computing. National Institute of Standards and Technology.

Moores, T. (2005). "Do consumers understand the role of privacy seals in e-commerce?" *Communications of the ACM* 48 (3)**,** 86-91.

Oezpolat, K., G. Gao, W. Jank and S. Viswanathan (2013). "The value of third-party assurance seals in online retailing: An empirical investigation." *Information Systems Research* 24 (4)**,** 1100-1111.

Petter, S., D. Straub and A. Rai (2007). "Specifying formative constructs in information systems research." *Management Information Systems Quarterly* 31 (4)**,** 623-656.

Podsakoff, P. M., S. B. MacKenzie, J.-Y. Lee and N. P. Podsakoff (2003). "Common method biases in behavioral research: a critical review of the literature and recommended remedies." *Journal of Applied Psychology* 88 (5)**,** 879-903.

Schneider, S. and A. Sunyaev (2016). "Determinant factors of cloud-sourcing decisions: reflecting on the IT outsourcing literature in the era of cloud computing." *Journal of Information Technology* 31 (1)**,** 1-31.

Sethi, V. and R. C. King (1999). "Nonlinear and noncompensatory models in user information satisfaction measurement." *Information Systems Research* 10 (1)**,** 87-96.

Shaked, A. and J. Sutton (1982). "Imperfect information, perceived quality, and the formation of professional groups." *Journal of Economic Theory* 27 (1)**,** 170-181.

Simonin, B. L. and J. A. Ruth (1998). "Is a company known by the company it keeps? Assessing the spillover effects of brand alliances on consumer brand attitudes." *Journal of Marketing Research* 35 (1)**,** 30-42.

Siponen, M. and A. Vance (2014). "Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations." *European Journal of Information Systems* 23 (3)**,** 289-305.

Smith, H. J., T. Dinev and H. Xu (2011). "Information privacy research: an interdisciplinary review." *Management Information Systems Quarterly* 35 (4)**,** 989-1016.

Smith, H. J., S. J. Milberg and S. J. Burke (1996). "Information privacy: measuring individuals' concerns about organizational practices." *Management Information Systems Quarterly* 20 (2)**,** 167-196.

Söllner, M., A. Hoffmann and J. M. Leimeister (2015). "Why different trust relationships matter for information systems users." *European Journal of Information Systems* 25 (33)**,** 274-287.

Straub, D. W. (1989). "Validating instruments in MIS research." *Management Information Systems Quarterly* 13 (2)**,** 147-169.

Sunyaev, A. and S. Schneider (2013). "Cloud services certification." *Communications of the ACM* 56 (2)**,** 33-36.

Tang, Z., Y. Hu and M. D. Smith (2008). "Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor." *Journal of Management Information Systems* 24 (4)**,** 153-173.

Xu, H., T. Dinev, J. Smith and P. Hart (2011). "Information privacy concerns: Linking individual perceptions with institutional privacy assurances." *Journal of the Association for Information Systems* 12 (12)**,** 798-824.

Xu, H., H.-H. Teo, B. C. Tan and R. Agarwal (2012). "Research note - Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services." *Information Systems Research* 23 (4)**,** 1342-1363.

Yamagishi, T. and M. Yamagishi (1994). "Trust and commitment in the United States and Japan." *Motivation and Emotion* 18 (2)**,** 129-166.

Yang, H. and M. Tate (2012). "A descriptive literature review and classification of cloud computing research." *Communications of the Association for Information Systems* 31 (2)**,** 35-60.

Zhao, X., L. Xue and A. B. Whinston. "Managing interdependent information security risks: A study of cyberinsurance, managed security service and risk pooling." International Conference on Information Systems. 2009 Phoenix. p. 49.