Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2013 Completed Research

ECIS 2013 Proceedings

7-1-2013

Cloud Service Certifications: Measuring Consumers' Preferences For Assurances

Jens Lansing
University of Cologne, Cologne, Germany, lansing@wiso.uni-koeln.de

Stephan Schneider
University of Cologne, Cologne, Germany, schneider@wiso.uni-koeln.de

Ali Sunyaev
University of Cologne, Cologne, Germany, sunyaev@wiso.uni-koeln.de

CLOUD SERVICE CERTIFICATIONS: MEASURING CONSUMERS' PREFERENCES FOR ASSURANCES

Lansing, Jens, University of Cologne, Albertus-Magnus-Platz, 50923 Cologne, Germany, lansing@wiso.uni-koeln.de

Schneider, Stephan, University of Cologne, Albertus-Magnus-Platz, 50923 Cologne, Germany, schneider@wiso.uni-koeln.de

Sunyaev, Ali, University of Cologne, Albertus-Magnus-Platz, 50923 Cologne, Germany, sunyaev@wiso.uni-koeln.de

Abstract

Cloud computing by now has gained wide recognition in business and is becoming increasingly important for consumers. However, consumers experience uncertainties, such as security, privacy, and vendor lock-in. Certifications provide assurances and may mitigate uncertainties, making cloud service certifications a core focus of the European Union's cloud strategy and various certification programs. In this paper, we identify ten potential assurances for cloud service certifications and empirically assess their relative importance as perceived by consumers. We surveyed 53 consumers who use or intent to use consumer cloud services in a discrete choice experiment that follows the best-worst scaling (BWS) method. Results indicate that privacy, security, and availability are the three most preferred assurances, whereas process maturity, flexibility, and financial stability are the three least preferred assurances. This paper contributes to research by utilizing BWS, which – to the best of our knowledge – so far has not been used in IS research, and thereby directing attention to a promising method. By identifying and empirically ranking various quality and trust assurances for consumer cloud services, we furthermore build foundations for future research on trust-assuring arguments and quality signals for cloud services as well as provide insights for practice on designing effective cloud service certifications.

Keywords: Cloud computing, certification, trust, best-worst scaling.

1 Introduction

Cloud computing is among the most important strategic technologies and has the potential to change the way information technology (IT) is used within the next ten years (Gartner Research, 2012a). Cloud computing is an IT deployment model that provides on-demand network access to a shared pool of managed and scalable IT resources on a pay-per-use basis (Mell and Grance, 2011). By 2016, consumers are expected to store more than a third of their digital content in *the cloud* (Gartner Research, 2012b). However, regarding the adoption of cloud computing, consumers still face uncertainties concerning for instance security, privacy, or vender lock-in (Li and Chang, 2012). Users have relatively few means to assess which providers offer high quality services and are trustworthy (Sunyaev and Schneider, 2013). Discussions on legal conflicts between the United States Patriot Act and the European Union (EU) Data Protection Directive 95/46/EC (Whittaker, 2011) as well as service terms like Amazon's further intensify the uncertainty: "*We may change, discontinue, or deprecate any of the Service Offerings (including the Service Offerings as a whole) or change or remove features or functionality of the Service Offerings from time to time.*" (Amazon Web Services, 2012)

Reflecting the uncertain cloud computing environment through the lens of signaling theory (Spence, 1973), the current market lacks credible signals to mitigate consumers' adoption uncertainties. Trust has been identified in multi-disciplinary research as a key signal to mitigate an interested party's uncertainty. IS research considers trust especially important in online contexts, because it mitigates uncertainties related to the online medium, such as security and privacy or seller integrity (Pavlou et al., 2007). Within the e-commerce context, higher levels of trust are associated with price premiums (Ba and Pavlou, 2002) and increased purchasing intentions (McKnight et al., 2002). Applied to the cloud computing context, certifications of cloud services or providers aid as signaling instruments for high service quality (Praeg et al., 2006) and are supposed to engender trust in cloud services (Khan and Malluhi, 2010; Sunyaev and Schneider, 2013). Compared to the outlined extant research, cloud services belong to a different product category. In e-commerce, certifications address concerns about sellers rather than products sold online. For cloud services, a certification needs to address concerns about the provider as well as concerns about the product (the service itself). This is why organizations such as Cloud Security Alliance and EuroCloud initiated cloud certification programs for individuals, providers, or services and the recently published EU cloud computing strategy defines developing cloud-specific certifications as a key action (European Commission, 2012).

However, findings on the effect of certifications or seals on trust or adoption behavior are inconclusive (Hu et al., 2010; Kim and Benbasat, 2009; Lowry et al., 2012). Certifications are issued if an organization, a product, or a service fulfills a predefined set of criteria after undergoing an audit by a third-party institution. Hence, a certification may be conceptualized as a set of third-party "trust-assuring arguments" (Kim and Benbasat, 2009). The effect of these arguments on consumers' beliefs, attitudes, and behaviors are determined by content of an argument, source of an argument (i.e., the party issuing the statements) and contextual factors influencing consumers' perceptions of an argument (Kim and Benbasat, 2009), such as product category and price, risks or personal relevance. Thus, certifications will only be effective if they are properly designed for a specific product or service and – depending on expertise and personal preferences – users may assign differing importance to assurances of certifications. Recent research (e.g., Praeg et al., 2006) and results of our interviews (cf. section 3) indicate that security and privacy are not the only assurances that need to be provided by effective certifications. However, most existing cloud service certifications focus on security or privacy.

Despite calls for developing (European Commission, 2012; Khan and Malluhi, 2010) and investigating the efficacy of signals such as certifications in the cloud computing context (Venters and Whitley, 2012), there is currently a dearth of research on the effective design of cloud service certifications. As a first exploratory study towards better understanding cloud service certifications, this paper answers the following research questions: *What assurances do cloud service certifications need to provide and what is the relative importance of identified assurances as perceived by consumers?* To answer these questions, we first derive ten assurances from extant literature, expert interviews, and existing cloud service certifications. To determine the relative importance of each assurance, we evaluate results from a discrete choice experiment that follows the best-worst scaling (BWS) method.

The remainder of this paper is structured as follows. First, we provide a theoretical overview on the signaling and trust-assuring role of certifications. Next, we introduce ten assurances for cloud service certifications. We then present the research method of our empirical study followed by the results. This article ends with a discussion of findings and a conclusion.

2 The Signaling and Trust-Assuring Functions of Certifications

Following extant literature (e.g., Kimery and McCord, 2006), certifications can be analyzed by signaling theory and trust theory. 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. Signals must be costly to be effective (Spence, 1973). To obtain a certification, an organization must undergo an audit process conducted by a third-party institution in which fulfillment of a set of predefined criteria is tested. Within IS research, certifications are thus signals that are intended as means to influence a customer's beliefs, attitudes and behaviors (Kimery and McCord, 2006). From a trust theory point of view a certification is a set of "trust-assuring arguments" (Kim and Benbasat, 2006) or a structural assurance which contributes to formation of trust via institution-based trust (McKnight et al., 2002). Trust is defined as "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" (Rousseau et al., 1998, p. 395). McKnight et al. further define trusting beliefs, which "means the confident truster's perception that the trustee […] has attributes that are beneficial to the truster" (2002, p. 337). Institution-based trust is an antecedent of trust and means "the belief that needed structural conditions are present (e.g., in the Internet) to enhance the probability of achieving a successful outcome in an endeavor like e-commerce" (McKnight et al., 2002, p. 339).

IS research investigates certifications from both signaling and trust perspectives. For example, within the IT offshoring industry, the quality signal communicated by a capability maturity model (CMM) certification is expected to reduce information asymmetries and is associated with higher export revenues of certified firms (Gao et al., 2010). The majority of IS research on certifications and seals, however, focuses on trust between buyers and sellers in the e-commerce domain. Predominantly investigated certifications are information privacy (e.g., Kim and Kim, 2011), 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). Interestingly, despite the strong theoretical foundation, empirical findings on the effect of certifications on consumers' beliefs, attitudes or behaviors as well as the trust-engendering effect so far have been inconclusive. While some studies find a significant effect of certifications or seals on trust (e.g., Hu et al., 2010; Kim and Kim, 2011), others do not find a significant effect of certifications or seals on trust (e.g., Kim et al., 2008; McKnight et al., 2004). Comprehensive overviews of disparate findings of extant research on certifications are provided by Lowry et al. (2012) and Hu et al. (2010). However, these inconclusive findings do not necessarily imply that certifications are irrelevant, but the effect of certifications rather depends on contingency factors (Kim and Benbasat, 2009; Lowry et al., 2012). As stated above, these factors are content of an argument, source of an argument and contextual factors influencing consumers' perceptions of an argument (Kim and Benbasat, 2009). Trust theory suggests that trust is built by cognitive processes (e.g., prediction, intentionality and transference; cf. Doney and Cannon, 1997). Using these processes as analytical devices, content and source factors of certifications can be explained (Kim and Benbasat, 2006).

From a content perspective, trust-assuring arguments communicated by a certification exert a direct effect on users' trusting beliefs by addressing customers' beliefs in a vendor's characteristics (e.g., competence, benevolence, integrity; cf. McKnight et al., 2002) or an indirect effect by influencing antecedents of trusting beliefs such as privacy and security concerns (Kim and Benbasat, 2006). Both effects result from prediction and intentionality processes (cf. Kim and Benbasat, 2006, p. 290): a certification contains information on a provider's practices (e.g., regarding information privacy protection) as well as promises (e.g., adherence to a specific code of conduct), and thus provide additional informational cues for customers to evaluate a provider's intentions and to predict a provider's future behavior. There is evidence that a trust-assuring argument's influence on trusting beliefs is contingent upon the type of argument content and its form of presentation. For example, privacy assurances, security assurances and integrity assurances have differential effects on trusting beliefs (Hu et al., 2010). Furthermore, when including multiple assurances in one seal the overall level of trusting beliefs starts to decrease after including a specific number of assurances and thus follows an inverted U-shape (Hu et al., 2010). Finally, Kim and Benbasat (2006) find trust-assuring arguments lead to increased trusting beliefs when claims are supplemented by data as grounds for a claim as well as backings for "why data should be accepted" (p. 286).

From a source perspective, a certification may initiate a trust transference process. Assuming that a certification authority is trustworthy to a consumer, a certification may establish a cognitive association between a certified provider and a certification authority, by which a consumer's trust in a certification authority is transferred to a certified provider, reducing the consumer's concerns. Empirical evidence supports this proposition. For example, Nöteberg et al. (2003) find that third-party assurances communicated via a certification seal lead to lower privacy and integrity concerns compared to vendor-provided assurances and no assurances. However, the study finds no significant differences between different third-party assurance providers. The results are confirmed by Kim and Benbasat (2009), although interestingly, for high-price products a web vendor's self-proclaimed assurance that follows the aforementioned claim-data-backing scheme has a higher effect on higher trusting beliefs than a third-party assurance that only includes claims.

Last, the trust-engendering effect of certifications is contingent upon contextual factors (Kim and Benbasat, 2009), such as vendor and product familiarity, product category and consumer involvement. For example, Mauldin and Arunachalam (2002) only find a significant effect of assurance seals on purchase intentions when product familiarity was low and disclosures provided by retailers on their business practices were not observed. Furthermore, different types of certifications have differential effects for different product categories. While information assurance seals only increase willingness to buy for search goods, reliability assurance seals increase willingness to buy for both search and experience goods (Zhang, 2005). Kim and Kim (2011) experimentally find that a well-known privacy seal engenders trust in vendors unfamiliar to consumers only if purchase involvement is low.

In sum, research by now provides nuanced insights on the conditions under which certifications may engender trust and work as quality signals: First, certifications need to convey assurances which address concerns relevant for the product category at hand and which are properly designed. Second, assurances provided by certifications need to influence trusting beliefs – either directly or indirectly via trust antecedents. Finally, to be costly, certifications need to be issued by a trustworthy authority. As an initial step towards designing effective cloud service certifications, we focus on the first principle and derive assurances that are most relevant to cloud consumers from extant research and practice.

3 Assurances of Cloud Service Certifications

We followed a three-step approach to determine assurances relevant for cloud service certifications. First, we derived an initial set of assurances from extant literature on certifications. Second, we searched the literature on cloud computing for cloud-specific challenges that form current customer concerns. Third, in order to discuss, refine, and above all validate the derived certification assurances, we conducted thirteen expert interviews between June and September 2012. We interviewed users, providers, and consultants involved in cloud-related decisions within their organizations. Whenever possible, we conducted the interview with the executive level. We analyzed the interviews by iterative descriptive and interpretive coding (Myers, 2009) since data collection was continued throughout the study. We asked interviewees for assurances that should and should not be included in a cloud service certification and coded the interviewees' attitudes to the assurances (positive, neutral, or negative).

Assurance	Definition
Availability	The provider complies with performance commitments, ensures availability of data, and operates measures to prevent data loss.
Contract	The provider offers understandable contractual arrangements that meet common business practice and the contract terms do not restrict the customers' property rights of their data stored in the cloud service.
Customer Support	The provider ensures accessibility and responsiveness of the customer support and practices a proactive information policy towards customers.
Financial Stability	The medium-term financial viability of the provider is assured.
Flexibility	The customer can independently adjust the obtained capabilities and the adjustments are carried out automatically within a short period of time and with transparent costs.
Interoperability	Customers can save and export data in standard formats, the cloud service offers open interfaces for integration with other cloud services or applications, and customers can access the cloud service location-independently via various devices.
Legal Compliance	The provider complies with legal and regulatory requirements of cloud services.
Privacy	The provider complies with applicable data protection laws, refrains from content-related analysis of the customers' data stored in the cloud service, completely and unrecoverably deletes all customer data after termination of the contract, and does not sell, rent or give away customer data to third parties.
Process Maturity	The business processes maturity of the provider aligns with established best practices in the IT service sector.
Security	The provider has established measures to ensure that data is securely stored, transmitted and protected against unauthorized access by third parties and other cloud service users.

Table 1. Definitions of assurances.

Using the set of potential assurances, two researchers independently formed categories. Primary goal was to derive a set of assurances, which are mutually exclusive and theoretically map to either trust dimensions or empirically proven trust antecedents (e.g., Goo et al., 2009; McKnight et al., 2011; McKnight et al., 2002). A comparison of categories resulted in minor discrepancies, which were discussed and resolved. As a quality check, we mapped the derived assurances against existing cloud service certifications, which resulted in no additional assurances. Applying this methodology resulted in ten assurances for cloud services (cf. Table 1).

Assurance	Research						Existing cloud certifications							Interviews			
	Armbrust et al. (2010)	Badger et al. (2012)	Browning and Macdonald (2011)	Marston et al. (2011)	Praeg et al. (2006)	Susarla et al. (2010)	Cloud Security Alliance, STAR	EuroCloud, EuroCloud Star Audit	EuroPriSe, European Privacy Seal	General Services Administration, FedRAMP	SaaS-EcoSystem, Trust in Cloud	TRUSTe, TRUSTed Cloud	TÜV Rheinland, TÜV Cloud Security	Positive (%)	Neutral (%)	Negative (%)	Total Responses (Count)
Availability	x	x	x		x	x		x			x			100	0	0	7
Contract		x		x	x			x			x			80	0	20	5
Customer Support					x			x			x			50	0	50	4
Financial Stability	x	x	x	x	x			x			x			50	0	50	8
Flexibility	x	x						x			x			100	0	0	1
Interoperability	x	x	x	x				x			x			75	25	0	4
Legal Compliance	x	x	x	x	x			x			x			88	13	0	8
Privacy		x	x	x		x		x	x		x	x	x	80	20	0	5
Process Maturity					x	x		x						100	0	0	6
Security	x	x	x	x	x	x	x	x		x	x		x	100	0	0	12

Table 2. Assurances suggested by research, existing cloud certifications and interviews.

Table 2 provides an overview of the ten identified assurances and their corresponding representation in research, existing cloud certifications and interviews. Existing certifications vary, among other aspects, by provided assurances. Most current cloud service certifications focus on security and privacy, which is in line with major concerns of (potential) cloud users. However, our results indicate that security and privacy are not the only assurances that need to be provided by effective certifications.

4 Method for Empirical Preference Measurement

To assess the relative importance of assurances, we next conducted a discrete choice experiment that follows the BWS method (see section 4.1). Before deploying the final experiment, we conducted a pre-test with eight graduate MIS students and a pilot survey with 14 undergraduate MIS students. The pre-test was primarily intended to assess comprehensibility of instructions and face validity of the selected ten assurances and resulted in wording changes to assurance descriptions and instructions, as well as layout changes. The pilot test provided a preliminary assessment of the relative importance of the ten identified assurances, which strongly encouraged us to proceed with the final survey. After the pilot test, we applied minor wording changes to the instructions and carefully re-specified the order of appearance of items within each choice set to avoid any potential order effects (see section 4.2).

4.1 Best-Worst Scaling

BWS was introduced by Finn and Louviere (1992) as a method to measure concerns or preferences regarding attributes and – optionally – levels of attributes. Basically, BWS is a special type of discrete choice experiment. As with regular choice experiments, respondents are repeatedly presented a set of three or more choices, which may be either attributes (so-called Case 1 experiment), varying levels of attributes (Case 2 experiment) or profiles of attributes that differ by attribute levels (Case 3 experiment). But instead of choosing one option (usually the most preferred) from each of these choice sets, respondents are required to make two choices by deciding upon the most preferred *and* the least preferred option. Using observations obtained from all choices of all participants, preferences for each attribute and attribute level can be calculated using a simple scoring mechanism or a conditional logistic regression (see section 5). In addition to Finn and Louviere (1992), who investigate importance of public concerns, example applications of BWS include measurement of values (Lee et al., 2007) or measurement of consumer ethical beliefs (Auger et al., 2007). To the best of our knowledge, we are the first to apply BWS in IS research. Due to size limitations, we only provide a brief overview on the method and underlying assumptions and refer to Flynn (2010) for an introduction to BWS, Flynn et al. (2007) for a detailed guideline on how to conduct BWS experiments, and Marley and Louviere (2005) for mathematical foundations of BWS.

As our intention is to derive consumer preferences for assurances provided by cloud service certifications, and not levels of assurance, we deployed a Case 1 experiment, and leave investigating preferences for assurance levels for future research. Resulting data can be used to derive a preference ranking. Compared to traditional preference elicitation methods, such as rating scales (e.g., a Likert scale) or other discrete choice tasks, BWS has several advantages: it allows obtaining a high level of ranking information because each decision for a pair of attributes contains implicit information on the not-chosen attributes (Marley and Louviere, 2005); it is scale-free and thus avoids “response styles, which can affect both the mean and the variance obtained” (Lee et al., 2007, p. 1044) and – unlike rating scales – forces respondents to make discriminating choices. Furthermore, other potential response biases can be avoided (Lee et al., 2007, pp. 1044–1046). Comparisons of BWS with ranking or rating methods demonstrate that BWS provides superior results with regard to discrimination between attributes (indicated by lower and lesser number of significant correlations; cf. Lee et al. 2007).

BWS builds upon a classic random utility choice model that is extended by adding a second choice to each choice situation (cf. Marley and Louviere, 2005). For BWS two generic psychological models for the pair-choices exist (Flynn, 2010; Marley and Louviere, 2005): the so-called MaxDiff model proposed in the original BWS article, which assumes a "cognitive process by which respondents repeatedly choose the two objects in varying sets of three or more objects that they feel exhibit the largest perceptual difference on an underlying continuum of interest" (Finn and Louviere, 1992, p. 13). Hence, the underlying assumption is that respondents cognitively process all possible pairs of best-worst choices. Alternatively, a sequential choice model may be assumed (Marley and Louviere, 2005), which models a cognitive process by which respondents first choose the most preferred attribute and then choose the least preferred attribute (or vice versa). We evaluate both models in our analysis.

4.2 Experiment Design and Data Collection

The survey consisted of three steps: participant framing, choice experiment and validation task. In addition to these tasks, we asked for demographics. The framing step was supposed to assure a common baseline understanding of all participants. Participants were told that the survey's purpose was to gather opinions on a potential cloud service certification's contents. First, participants were given definitions of cloud services (based on Mell and Grance, 2011) and cloud service certifications (cf. section 1). Next, participants were instructed to assume that they are in an adoption decision for a consumer cloud service that is certified with a cloud-specific certification, which participants may consider in their decision. Participants were told that they will be presented 15 sets of four possible assurances (see below) and were asked to select the most and the least preferred assurances from the set of the four shown assurances. To avoid response bias, we did not refer to any particular assurance or mention any uncertainties that the selected assurances are supposed to mitigate in the framing explanations.

We asked participants to make choices under four assumptions. First, to stress signaling theory's proposition that signals must be costly, we stated that certification fees are paid by cloud service providers. Second, to address the source aspect of trust-assuring arguments, we stated that an independent and reputable organization conducts the audit based on an open standard. Third, to foster credibility of certification as suggested by our interviews, we stated that the certification requires an on-site audit and a review of documents provided by cloud service providers. Fourth, auditors only have a limited time frame for conducting the audit and cannot consider all assurances in exhaustive detail. The latter assumption was stated to ensure respondents consider making trade-offs between potential assurances.

In the choice experiment, each respondent was shown 15 unique choice sets of four items. The choice sets were created to jointly build a balanced incomplete block design. Thus, each item appeared an equal number of six times and each combination of two items was shown exactly twice. In deploying this design, we followed the guidelines developed by Orme (2005), who demonstrates that respondents should not be shown more than four to five items per choice set as well as each choice set should contain less than half of total items. Furthermore, there is a minimum required threshold of three observations per item and respondent and for studies with ten or less items a number of 15 tasks per respondent is sufficient (Orme, 2005). To avoid any order effects, we ensured that each assurance was shown at each position in the choice sets as recommended by Cohen (2003). Definitions of assurances were provided with each choice set for the four shown assurances.

The validation task asked participants to rank six of the ten assurances (availability, customer support, financial stability, interoperability, security, privacy). We selected these six assurances because we expected them to fully span the importance spectrum based on the pilot survey. Of course, one could argue that asking participants to rank all ten assurances would be an easier procedure than conducting a BWS experiment. However, we think that BWS provides a much more accurate solution: first, answering BWS is easier for respondents because each choice task has lower complexity than ranking ten assurances; second, due to repeated forced trade-off decisions between assurances, a BWS experiment will more accurately reflect the latent importance scale than a one-off ranking task.

Respondents for the main survey were recruited via a social network asking for participants who use or intent to use consumer cloud services. Participants were told to enter a raffle for a € 50 portable music device and a € 30 voucher for an online shopping website. Polls were closed after 7 days. 138

people followed the hyperlink to the survey and 53 respondents completely finished the survey, resulting in a response rate of 38%. Respondents' demographic characteristics are shown in Table 3.

	Age (years)	Gender	Occupation	Experience (years)		Cloud usage type
				Internet	Cloud[1]	
Average (STD)	26.9 (5.4)	19% female 81% male	2% pupil 6% apprentice 49% student 28% employed 11% self-employed 4% other	13.2 (2.5)	3.0 (2.2)	53% private use only 40% professional and private use 6% non-adopter 2% professional use only

Table 3. Respondents' demographic characteristics.

5 Results

Data were analyzed using R 2.15.1 with survival package 2.36-14. Results were calculated by a simple counting analysis and two variations of a conditional logistic regression, one for each of the two described cognitive processes. For the counting analysis we calculated a score for each assurance for each respondent by counting the number of times each assurance was chosen as most and as least preferred and dividing the difference by the number of times each assurance was shown (six times). The resulting scale ranges from -1 to +1 with a higher score implying that an assurance is more important to the respondent. Table 4 shows means, standard deviations and skewnesses on an aggregate level as well as the overall counts for each assurance. As Marley and Louviere (2005) proved and Orme (2009) showed empirically, the counting procedure provides results that are a close approximation of the results of a conditional logistic regression. We nevertheless conducted the latter analysis.

Assurance	Counting Analysis					Conditional Logistic Regression				Rank
	Mean	STD	Skew-ness	Overall Counts		MaxDiff Model		Sequential Model		
				Most	Least	Coef.	SE	Coef.	SE	
Privacy	0.63	0.35	-0.74	205	6	3.20	0.16	3.27	0.16	1
Security	0.51	0.33	-0.59	170	9	2.85	0.16	2.86	0.16	2
Availability	0.40	0.37	0.21	135	8	2.55	0.15	2.54	0.15	3
Interoperability	0.08	0.45	-0.42	89	62	1.59	0.14	1.62	0.15	4
Contract	-0.02	0.38	0.25	50	56	1.50	0.14	1.40	0.14	5
Legal	-0.12	0.40	-0.13	46	85	1.08	0.13	1.13	0.14	6
Customer Support	-0.16	0.48	0.26	54	105	1.02	0.13	0.99	0.14	7
Process Maturity	-0.34	0.37	0.03	19	126	0.55	0.13	0.61	0.14	8
Flexibility	-0.42	0.38	0.48	20	152	0.37	0.13	0.38	0.14	9
Financial Stability	-0.56	0.31	0.58	7	186	-	-	-	-	10
All regression coefficients are significant at p<.001, except Flexibility (p<.01)										

Table 4. Descriptive statistics for best-worst scaling data.

Both the MaxDiff model and the sequential model can be analyzed by a conditional logistic regression using a maximum-likelihood estimation of parameters. In modeling data for our analysis, we followed the guidelines by Flynn et al. (2007). For the MaxDiff model, we modeled one observation for each possible best-worse-pair per choice set per respondent. Assurances were modeled as independent variables and dummy-coded. A similar approach was followed for the sequential model. We modeled two

[1] Only includes respondents actually using cloud services (cf. column "cloud usage type").

observations for each assurance available per choice set per respondent, one for being chosen as most preferred, and one for being chosen as least preferred assurance in the choice set (except for the attribute chosen as most preferred). Assurances were again modeled as independent variables and dummy-coded. To avoid dummy variable trap, we chose one independent variable as the reference category, hence excluded it in both data sets (Hair et al., 2010). We decided for "financial stability" due to its lowest rank in the counting analysis. Coefficients and standard errors for each assurance are depicted in Table 4. As expected, a linear regression of scores and regression coefficients shows that results from all three analyses are similar (r^2=.9976 for counting analysis vs. MaxDiff model, r^2=.9977 for counting analysis vs. sequential model, and r^2=.9981 for sequential model vs. MaxDiff model).

Next, we assessed skewness of assurances and correlations between assurances. Skewness was assessed comparing the skewness statistic of each assurance with twice the standard error of skewness following Hair et al. (2010). Results indicate that of the ten assurances, only privacy is skewed. Correlations ranged from -0.53 to 0.4 and 40 out of the 45 correlations were not significantly different from zero at the 1% level (Table 5). Of the five significant correlations, four are negative and one is positive. Overall, we conclude that skewness is not a significant problem and respondents were able to meaningfully discriminate between assurances. Finally, to assess internal validity we compared assurances' scores with the ranking task results on an individual level. To calculate a "hit rate", we ranked the six assurances included in the validation task based on their counting scores and compared rankings with the validation task rankings on respondent level of analysis. The hit rate was 65.4%, which is common for BWS experiments (e.g., Orme, 2005, 2009).

No.	Assurance	1	2	3	4	5	6	7	8	9	10
1	Availability	1									
2	Contract	**-.48**	1								
3	Customer Support	.28	**-.48**	1							
4	Financial Stability	.31	-.23	.02	1						
5	Flexibility	-.01	-.07	-.08	-.10	1					
6	Interoperability	.03	-.04	-.23	-.15	-.05	1				
7	Legal	-.32	.11	-.25	-.31	-.29	-.32	1			
8	Privacy	**-.53**	.23	-.19	**-.38**	-.18	-.06	**.40**	1		
9	Process Maturity	-.05	-.07	.00	.02	-.30	-.03	-.11	-.26	1	
10	Security	-.32	.14	-.35	.01	.10	-.33	.18	.01	-.19	1
Note: bold correlations indicate p<.01											

Table 5. Correlation between assurances' scores.

6 Discussion and Conclusion

This study investigates consumer's preferences for assurances provided by cloud service certifications. Building upon the best-worst scaling method we empirically measure importance scores for ten potential assurances for cloud services. Results demonstrate that privacy, security and availability are the three most preferred assurances, whereas process maturity, flexibility and financial stability are the three least preferred assurances. Importance of security and privacy is consistent with extant research on certifications and seals in the e-commerce domain (cf. section 2) as well as our expert interviews. Results indicate that privacy is considered the most preferred assurance. This is not only due to the highest score and regression coefficients, but also supported by the negative skewness, which indicates that the majority of consumers rates data privacy with a higher than average score. The significant negative correlations with availability and financial stability indicate that consumers with a high preference for privacy assurance are less concerned about long-term availability of data, which may be a result of the commodity and thus interchangeability of consumer cloud services. Assurance of availability seems to be important in the cloud computing context, but has not yet been studied in IS research on certifications. This may be explained by the lesser amount of data exchanged in e-commerce, which has been prior focus of IS certification research. Typically, e-commerce transactions require provision and storage of address and billing information, which may easily be restored in case of data losses. However, cloud services often store pictures or other personal documents for which consumers' fears of loss are likely to be considerably higher. Overall, the results match our expectations based on the expert interviews conducted prior to the experiment. Interestingly, experts jointly agreed that process maturity is an important assurance, whereas experimental results indicate that it is of lesser importance to regular consumers. As process maturity is an assurance of provider integrity and reliability, this finding may indicate that integrity and reliability seals studied in e-commerce contexts (e.g., Hu et al., 2010; Zhang, 2005) are less important in cloud computing contexts.

This study has the following limitations. First, though our sample size of 53 respondents is sufficient to provide an estimate of cloud service consumers' preferences for assurances, it is relatively small. Hence, a larger sample might provide deeper insights. Second, there is little public information available on overall consumer cloud service user demographics. Though we are confident our respondent sample sufficiently matches the overall population and other recent studies on consumer cloud service acceptance have similar samples with regards to age and internet experience (e.g., Li and Chang, 2012), the actual population of consumer cloud service users might differ. Third, the relatively low share of female respondents might distort results. However, assessing potential gender impact on assurance preferences did not reveal any significant differences.[2]

A larger sample size would also allow exploring segments with differing assurance preferences. Extant research suggests that assurances are perceived differently by user segments, for instance experienced and inexperienced users (Zhang, 2005). Though an analysis of differences of assurances' scores between adopters and non-adopters did not show any significant differences[3], future studies might investigate other segments. A promising opportunity would be to explore assurance preferences across cultures. For example, a recent study comparing self-perception-based trust (e.g., security protection mechanisms) with transference-based trust mechanisms, a third-party seal, finds that the latter significantly influences trust for Korean respondents, but not for US respondents (Kim, 2008). Here, BWS is especially suited due to its independence of cultural scale interpretation (Auger et al., 2007).

Finally, our study provides insights on the relative importance of assurances, but does not provide insights on these assurances' influence on consumers' beliefs, attitudes or behaviors. Hence, future research should investigate whether and how the identified important assurances influence a consumers' beliefs (e.g., trusting beliefs, perceived uncertainties), attitudes (e.g., towards using a cloud service) and behaviors (e.g., usage of a cloud service). Given that the effect of certifications is highly contextual, evaluating certifications under different contextual conditions or comparing certifications to other quality signals or trust-assuring arguments are also promising research directions.

Contributions are threefold. First, by applying best-worst scaling, which so far has not been used in IS research, we direct attention to a promising method that might be used in other IS research domains. Second, by identifying and empirically ranking various quality and trust assurances for consumer cloud services, we provide foundations for future research on trust-assuring arguments and quality signals for cloud services. Third, practitioners can use our results to develop more focused certifications and to highlight most preferred assurances when communicating certifications to consumers.

Acknowledgement

The information in this document was developed in the context of the Value4Cloud research project, funded by the German Federal Ministry for Economics and Technology (FKZ: 01MD11043A).

[2] Mann-Whitney's U tests with male and female respondents as groups do not show any significant effect of gender on any of the ten assurances scores ($156 \leq U \leq 287$, $-1.37<Z<1.67$, $.09<p<.86$).

[3] Mann-Whitney's U tests with adopter and non-adopter respondents as groups do not show any significant effect of adoption on any of the ten assurances' scores ($52.5 \leq U \leq 115$, $-1.56<Z<.89$, $.13<p<.94$).

References

Amazon Web Services (2012). AWS Customer Agreement. http://aws.amazon.com/de/agreement.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53 (4), 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), 299–326.

Badger, L., Grance, T., Patt-Corner, R. and Voas, J. (2012). Cloud Computing Synopsis and Recommendations. NIST Special Publication 800-146. National Institute of Standards and Technology.

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

Browning, J.A. and Macdonald, N. (2011). Survey Analysis: North American Midsize Businesses Cite Cloud Intentions. Gartner Research. (Dataquest).

Cohen, S. (2003). Maximum Difference Scaling: Improved Measures of Importance and Preference for Segmentation. (Sawtooth Software Research Paper Series).

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

European Commission (2012). Unleashing the Potential of Cloud Computing in Europe. http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf.

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), 12–25.

Flynn, T.N. (2010). Valuing citizen and patient preferences in health: recent developments in three types of best–worst scaling. Expert Review of Pharmacoeconomics & Outcomes Research, 10 (3), 259–267.

Flynn, T.N., Louviere, J.J., Peters, T.J. and Coast, J. (2007). Best–worst scaling: What it can do for health care research and how to do it. Journal of Health Economics, 26 (1), 171–189.

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), 1012–1029.

Gartner Research (2012a). Gartner Identifies the Top 10 Strategic Technology Trends for 2013. http://www.gartner.com/it/page.jsp?id=2209615. Access: 2012-11-22.

Gartner Research (2012b). Gartner Says That Consumers Will Store More Than a Third of Their Digital Content in the Cloud by 2016. www.gartner.com/it/page.jsp?id=2060215. Access: 2012-11-13.

Goo, J., Kishore, R., Rao, H.R. and Nam, K. (2009). The Role of Service Level Agreements in Relational Management of Information Technology Outsourcing: An Empirical Study. MIS Quarterly, 33 (1), 119–145.

Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (2010). Multivariate Data Analysis. A Global Perspective. Pearson, Upper Saddle River, New Jersey, USA.

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), 407–418.

Khan, K.M. and Malluhi, Q. (2010). Establishing Trust in Cloud Computing. IT Professional, 12 (5), 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), 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), 175–206.

Kim, D.J. (2008). Self-Perception-Based Versus Transference-Based Trust Determinants in Computer-Mediated Transactions: A Cross-Cultural Comparison Study. Journal of Management Information Systems, 24 (4), 13–45.

Kim, D.J., Ferrin, D.L. and Rao, H.R. (2008). A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents. Decision Support Systems, 44 (2), 544–564.

Kimery, K.M. and McCord, M. (2006). Signals of Trustworthiness in E-Commerce: Consumer Understanding of Third-Party Assurance Seals. J. of Electronic Commerce in Organizations, 4 (4), 52–74.

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), 145–158.

Lee, J.A., Soutar, G.N. and Louviere, J.J. (2007). Measuring Values Using Best-Worst Scaling: The LOV example. Psychology & Marketing, 24 (12), 1043–1058.

Li, Y. and Chang, K.-c. (2012). A Study on User Acceptance of Cloud Computing: A Multi-Theoretical Perspective, In Proceedings of the Eighteenth Americas Conference on Information Systems.

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), 755–776.

Marley, A. and Louviere, J. (2005). Some probabilistic models of best, worst, and best–worst choices. Journal of Mathematical Psychology, 49 (6), 464–480.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011). Cloud computing – The business perspective. Decision Support Systems, 51 (1), 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), 33–54.

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 MIS, 2 (2), 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), 334–359.

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), 252–266.

Mell, P. and Grance, T. (2011). The NIST Definition of Cloud Computing. NIST Special Publication 800-145. National Institute of Standards and Technology.

Myers, M.D. (2009). Qualitative research in business and management. SAGE, Los Angeles.

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

Orme, B. (2005). Accuracy of HB Estimates in MaxDiff Experiments. Sawtooth Software, Inc. (Sawtooth Software Research Paper Series).

Orme, B. (2009). MaxDiff Analysis: Simple Counting, Individual-Level Logit, and HB. Sawtooth Software, Inc. (Sawtooth Software Research Paper Series).

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), 105–136.

Praeg, C.-P. Schnabel and U. (2006). IT-Service Cachet – Managing IT-Service Performance and IT-Service Quality, In Proceedings of the 39th Hawaii International Conference on System Sciences.

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), 393–404.

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

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

Susarla, Anjana Barua, Anitesh Whinston and Andrew B. (2010). Multitask Agency, Modular Architecture, and Task Disaggregation in SaaS. Journal of Management Information Systems, 26 (4), 87–117.

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

Whittaker, Z. (2011). Microsoft admits Patriot Act can access EU-based cloud data. www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225.

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