The usage of third party seals in e-commerce websites : Current implementation

Kasiran, MK and Meziane, F

Title	The usage of third party seals in e-commerce websites : Current implementation
Authors	Kasiran, MK and Meziane, F
Publication title	
Publisher	
Type	Conference or Workshop Item
USIR URL	This version is available at: http://usir.salford.ac.uk/id/eprint/2205/
Published Date	2004

The Usage of Third Party Seals in eCommerce Websites : Current Implementation.

Mohd Khairudin Kasiran and Farid Meziane

School of Computing, Science and Engineering
Salford University, Manchester M5 4WT, UK

Abstract: eCommerce is a faceless business arrangement where the process of creating trust towards merchants is still a big challenge. One of the methods that can be used to facilitate the creation of trust is through transference of trust from merchant to third party and then back to the consumer. This can be achieved by placing third party endorsements or seals on the merchants' websites. Currently, this method has been implemented in many web sites. Current evaluation on its implementation needs to be done due to its diversity and implementation integrity problems.

Keywords. Third party endorsement, seal, eCommerce, trust.

1. Introduction and Motivation

Virtual transaction via virtual market space requires different kind of trust compared to traditional commerce transaction. The inability to prove someone's physical presence and establish a direct relationship between two parties involved in the transaction makes the trust between them even more difficult to establish. Knowing that the barrier level for both parties to enter and leave the digital market space is very low, has prompted the two parties to assess the level of risk involved before trusting each other in an eCommerce transaction (Gary and Debreceny, 1998). However, a closer look at eCommerce transaction cycle shows that consumers are in a disadvantaged position especially if the product is non-digital and non-service product. Consumers are expected to fulfil their obligation first by committing their financial and information resources in the transaction before the merchants are able to proceed with their obligation. Therefore the requirement for establishing trust from consumers toward merchants will be a very important factor in an eCommerce market place setting (AICPA 1997; Daignault et al., 2002; Hoffman et al., 1999; Urban et al., 2000).

One of the methods that is being used to facilitate the establishment of trust in virtual market place is through institutional based trust which can be achieved by placing third party endorsements or seals on the merchants' websites (Noteberg, Christiaanse, and Wallage, 1999; Kovar, Burke and Kovar, 2000). Third party endorsements or seals provide some measure of protection from fraud for both consumer and retailer (Gritzalis and Gritzalis, 2001). As an introducer of the notion of "digital seals", Gritzalis and Gritzalis (2001) define the term as "a token, which is put on the e-commerce company's electronic assets, like the company's Web pages, and validates certain characteristics of the company itself, the services or the products offered by that company." In this paper the term third party endorsement and digital seals or seals will be used interchangeably. A great number of research have been carried out academically or professionally on the role and the effect of third party endorsement on web sites, but very few on the issues of its implementations. Therefore; this paper will look closely at the implementation of third party endorsement through digital seals placement on over 114 eCommerce websites. Hopefully the result will shed some light on the seal providers of the overall situation of seal industries especially on certain issues that have been picked up in this research, like maintaining the integrity of the seals. The consumers, on the other hand, will be made aware of the possibilities that vendors may exploit the third party seals to their benefit and how this situation can be avoided by checking the integrity of the seals. For this purposes, this paper will be divided into four sections. The first will concentrate on related studies and the background of third party endorsements. The next section will focus on the methodology of the research. This is followed by a section on discussion of the findings and finally the conclusion of the paper.

2. Brief Background of Trust

Trust is a fundamental element in business relationship regardless of its method of interaction. In current business setting, trust is created through the exchange of accepted legal financial instrument such as money that is guaranteed by the government or credit card and other debt instruments, which are being backed by financial institutions. eCommerce is a faceless business arrangement where all parties involved should have good relationship with each other. In order for a relationship to work for a long time, it must be accompanied by trust. eCommerce without relationship that is accompanied by trust is bound to fail. Trust is also important when risk is involved. Establishing trust then, is establishing the acceptances of risk. eCommerce is made possible by the development of Internet technology, therefore, creating trust in eCommerce is a

process of taking risk in believing that the Internet technology is able to function as expected for the purpose of eCommerce. In addition, creating trust in eCommerce environment is also accepting the risk that everybody involved in this faceless business environment will perform his or her duties as expected.

Knowing the basic property of trust is important in order to understand how trust is formulated and cultivated before it can be exploited on certain environment. The basic property of trust that is relevant to this research is that trust is not generally transitive but can be conditionally transitive especially at the early stage of trust relation development. According to Abdul Rahman (cited from McCullagh, 1998), this condition will allow certain form of trust to be transferred from one party to another. He suggests that the development of trust usually starts from recommended trust before transforms to direct trust. Recommended trust is a trust between two parties who have no experience dealing with each other and they rely on other parties' recommendation to develop the relationship. Meanwhile, direct trust is a trust relationship between two parties and the relationship is based on their experience dealing with each other in the past. Ideally, the best form of trust is one that is being created through direct relationship between trustee and trustor. Both of them would have first hand experience dealing with each other and learn how to trust the other parties over time (Cheskin Research /Studio Archetype, 1999). However, this situation is too ideal in a huge faceless eCommerce community on the Internet. Creation of trust especially at the early stage of relationship will be more effective through indirect trust or recommended trust. Since, both parties have no experience in dealing with each other and in the stage of calculus-based-trust or trust based on calculated risk, (Lewicki and Bunker, 1996) information from other trusted third party is important to support trust creation.

Several studies on third party endorsement have been conducted in the past by several researchers such as Anna Noteberg (1999), Noteberg, Christiaanse and Wallage (2000), Cheskin Research and Studio Archtype (1999) and Cheskin Research (2000). All of these researches conclude that third party endorsement has some impact on influencing consumers to proceed with the digital transaction. The influences of third party endorsement in creating trust toward merchant become more significant, especially to unknown merchants where the perceived risk is higher than well-known merchant like Amazon.com (Noteberg, Christiaanse and Wallage, 2000). In addition, third party assurances can also be very useful especially if they involve endorsement on expertise and skill.

Among major services that are being offered by the third party assurances are:
  i) verifying the legitimacy of the company (existence).
  ii) ensuring certain standard of network security has been put in place by the business organisation (performance).
  iii) acting as protector to the consumer if something goes wrong in the transaction (policy/procedure).

Third party endorsement providers may come from government or private base organizations and offer a wide range of assurances such as quality assurance, code of conduct, code of practice, rating service, privacy etc. Some of these providers require fee from merchants for using their assurance seals in the merchant's website but some of them provide the service without any charges.

3. Objectives

The objective of this research is to look closely at current implementation of third party endorsements in eCommerce websites. Knowing the significant role of this institutional based trust in influencing trust creation, some kind of evaluation need to be carried out from time to time on its implementation. Among the questions that will be answered through this work are:
- How many sites have third party endorsements?
- What are the endorsements that are being used?
- What are the services that are being offered by the endorsers?
- Who are the providers?
- Is there any method for the consumer to verify the validity of the endorsements used?

4. Method

A list of 125 potential eCommerce websites were selected using several shoppingBoat such as mySimon, Dealtime, StoreRunner,Best Book Buy, BizRate, BottomDollar, BuyBuddy, Cnet, DealCatcher and DestinationRX while window shopping on several product such as electronic equipment, book, medicine, computer, chocolate, shoes, tools and household products. Out of these 125 websites, 11 of them were no longer available during the course of the research. The reason why they were no longer available was beyond the research scope. Therefore, the total websites that had been used in this research were 114. These websites were closely monitored to determine if there was any presence of third party endorsement seals on their websites as in figure 1.

Figure 1: An example of eCommerce storefront with several third party seals implemented on the web sites.

By using content analysis method, these seals were selected by clicking on them in order to answer the research questions mentioned above. In addition two sets of data

were collected at two different point of time. The first set of data was collected from January to April 2002 and the second was collected from August to December 2003.

5. Results and Discussion

1. How many sites have third party endorsements?

As indicated in the literature, institutional based trust has a very influential role in triggering consumer transaction in eCommerce. The presence of a third party endorsement or a seal has prompted a convincing environment to customer toward completing online transaction. This situation has been exploited by more than half of the online merchants included in the research. Based on the 2002 and 2003 data, out of 113 websites (n=113), 74 websites (65 %) had placed third party seals on their websites and 39 websites (35 %) did not have any third party seals. Even though it seems that the number of websites that used third party seals did not change, a closer examination on the data revealed that there was a reason for this situation. In 2002, several websites used the seals illegally or used unverified seals and they had been withdrawn in 2003. This situation had reduced the number of websites that had third party endorsement in 2003. However this reduction had compensated by the new websites that started to use third party seals in 2003. In other words, statically the number of websites that had endorsement did not change but in reality as expected there were several new websites that started to use third party seals. The same conclusion can also be made if we were to look at the overall number of seal available in the websites. 192 seals were available in 2002 and 204 seals in 2003. There were also 4 new types of seal being found in 2003. However, there were also 4 seals that available in 2002 but were no longer available in 2003.

Out of these 74 websites, the number of endorsement on each web site was different ranging from one to nine seals. 36 out 74 websites (48 %) that had endorsement used more than 2 endorsements on their websites in 2002 and 38 out of 74 (53 %) websites in 2003. There are several reasons for one website to have more than one seals. Certain type of third party seals carry different type of endorsement such as privacy adopted, technology usage or children protection. Therefore, in order to get the maximum effect of using third party endorsement, the websites are using more than one third party endorsements. Clearly, the possibility for a consumer to trust a website that has more than one third party endorsement is higher. Therefore, the chance for creating trust relationship is better than those websites with less endorsement.

2. What are the endorsements that are being used?

Among endorsement that were found in the websites and the corresponding number of websites that used them in 2002 and 2003 are Verisign (38,39), Bizrate (35,33), Cnet (9,9), BBB (27,29), TrustE (12,11), CyberSource Protected Buy (1,3), TrustWiseBT/COMMODO (1,0), TechSelect (2,1), JVC (3,3), JBT (2,2), DMA (2,1), TestedForSafety (1,0), Web Assured (1,0), Thawte Authentic Site (5,5), Hacker Safe (4,8), Reseller Rating (1,1), Authorized Reseller (1,1), ICRA (1,1), IMRG/ISIS (1,1), GeoTRust (1,2), PayPal (3,3),

VIPPS (1,1), Safe Shopping Network (2,2), Certified Merchant (1,0), Amex Fraud Protection (2,3), MasterCard Code (0,1), Verified by Visa (2,2), Ask Jeevs Preferred Retailer (1,1), Dyson Dealer (1,1) Sony Cert. Dealer (4,3), Forbes Favourite (2,2), Epic Org (1,1), Public Eye (1,1), Epinion (1,2), Price Assured (1,5), AOL Certified Merchants (3,5), Deal Time Certified (4,4), MySimon Certified Store (2,1), Yahoo Featured merchant (8,5), Gomez Certified (4,2) and Price Grabber User Rated (0,5).

Figure 2: Example of several seals that available in the eCommerec web site used in this research.

Based on the statistic provided above Verisign (38,39), Bizrate (35,33 sites) and BBB (27,29) were the most commonly used endorsement by the eCommerce merchants. These 3 endorsers provide different kinds of endorsement. Versign is more on verifying the merchant and verifying the security technology used such as SSL implementation. Bizrate is more on providing evaluation on the merchant reputation through its independent space for consumer comment and feedback. Meanwhile, BBB provides store verification and customer dispute resolution. These three endorsements do not change much in term of total websites that use them within the time period of this research. Verisign and BBB have increased but Bizrate has decreased probably due to unfavourable comments from consumers that lead to the merchant withdrawing the usage of this seal on their websites. Meanwhile the usage of several seals such as HackerSafe (4,8), Price assured (1,5) and Price Grabber User Rated (0,5) has increased significantly. The usage of HackerSafe endorsement is to emphasize the security factor in the web site implementation since most of the website that use this endorsement also use Verisign endorsement. PriceAssured endorsement has been used by website that sell electronics and camera to which price factor is very important to attract potential customers.

3. What are the services that are being offered by the endorsers?

There are different ranges of service that being provided by these third party endorsements. Endorser like Verisign, CNet, BBB (reliability Program), COMMODO, Web Assured, Cnet, IMRG (ISIS)and several others provide merchant verification in terms of identity and site authentication. Meanwhile, endorsers like TrustE, Epic.Privacy, DMA and BBB (Privacy) have examined the privacy policy of the merchant and verified as meeting their standard of privacy protection. There are also several endorsers that endorse the technology used by the websites. For example, Thwate, Verisign (secure site), COMMODO,

Tested for Safety, GeoTrust and TechSelect verify the security technology used such as SSL or PKI implementation. There are also a number of endorsements that have endorsed the site by providing independent space for maintaining feedback and complain about the merchant. The endorsers are Bizrate, ResellerRating, Price Grabber User Rated, Shopping.Com, MySimon, DealTime and Eponion. Their endorsement is based on the feedbacks provided by consumers about the store to them. In addition, there are also providers such as BBB, who are willing to be a mediator to unresolved problem between consumer and the merchant. There are also endorsements which are only available to a specific industry such as pharmaceutical or jewellery industry. Endorsement like JVC and JBT are specific for jewellery Industry where they endorse the code of conduct of the store as well as the authenticity of the product sold by the store. Meanwhile VIPPS endorsement is specific to pharmaceutical industry whey endorsement are made on verified store identification, patient rights to privacy, authentication and security of prescription orders.

Certain seals carry many endorsements through the same seal such as PublicEye who carries different endorsement like reliability, privacy and consumer satisfaction endorsement. Others seals, such as Verisign (Secure Site, Trusted Network and Authentic Site) and BBB (Reliability Program, Market Place Ethics and Privacy) carry different endorsement through different seals. The services provided by them through one seal can either be in only one area or in many areas.

4.   Who are the providers?

These endorsements are provided by both private companies and semi governmental organizations. These two providers can generally be classified as profit and non-profit entities. Both providers generally have the same goal, which is to help establishing trust through their certification. They want consumer to have confidence in the eCommerce channel. While private companies, which are more profit oriented, will charge the business organization to use their seal certification, non-profit organization will allow business organization to use their seal certification with minimal fees. Verisign for example is owned by VeriSign Inc, a listed company at NASDAQ, gives the Verisign seal freely with the implementation of SSL certificate which will cost from USD 349 to USD 1595. While BBB owned by Council of Better Business Bureau in the United States and Canada, provides the seals with the cost tied to the annual sales of the company. "A company with USD 1 million or less in total company sales would pay a one-time application fee of USD 75 and an annual assessment evaluation fee of USD 150 (ranging to USD 5,000 per year for companies with over USD 2 billion in annual sales)". The same method of charging is also being used by TrustE owned by a San Jose California - based privacy advocacy group, except that they use total revenue as a basis of calculation. The fees can range from USD 599 to USD 75,000 per year. Meanwhile, other endorsement such as HackerSafe owned by ScanAlert can cost the merchant from USD 1,790 per year.

5.   Is there any method for the consumer to verify the validity of the endorsements used?

The issue of verification is very important in this research since there are cases for each endorsement where their authentication is in question. Having endorsement that cannot be verified can give negative effect to the site. A case like http://www.photoalley.com/ or http://www.pagecomputers.com/ where they have several endorsements on their websites, which cannot be verified, can give a wrong massage to consumer about their business ethics in general * (The test has been conducted on 12-02-04 at 1.00 pm GMT). In addition, unverified seals also caused integrity problem on the seal itself since seal can be copied by unauthorized merchant on their web site.

There are different levels of verification that are being used based on the seals available in this research. The strictest verification is where the seals provide the mechanism to check the validity of the seals used on the websites. The seal provider will provide a verification of its seals through its secured server when consumers click on the seals that are available on the merchant's websites. For example, Verisign will show an online certificate that shows whether the seals are valid, revoked or expired. If the consumer clicks on the seals and no certificate is being shown then the consumer can assume that the seal has been used illegally without proper authorization. As a result, with this kind of verification the provider can easily maintain the integrity of the seals. Based on the data of this research, out of 38 seals on Verisign, there are 6 of them that cannot be verified. These endorsements are in question since Verisign has specifically mentioned that a legitimate endorsement should be linked to a certificate that can be validated through their server. Verisign is not the only one with this problem. 6 out of 25 for Bizrate and 1 out of 23 for BBB are having the same problem of invalidated endorsement. The endorser will not guarantee the conduct and the information provided in the web sites if the certification couldn't be validated or being used illegally.

There are also other methods that are being used by other seals in order to maintain their credibility and integrity. COMMODO, for example, not only provides some kind of certification on its seals but also provides compensation on any wrong information that they have provided. They provide a cover up to USD 10,000 compensation insurance for inaccurate information that they provide on the certificate, which caused lost on the consumer side. Meanwhile, seals like Bizrate, Safe Shopping Network, Eponion and several other comparisons shopping service providers depend on the feedbacks and comments from other consumers who have direct experience dealing with the merchants. They only provide the independent and non-bias publication of these feedbacks and comments linked to their seals. They have certain rules and method to conform to before they can give permission to certain ecommerce websites to use their seals. Price Grabber for example only allows those that have bought something from that merchant to make a review on that particular merchant (http://www.pricegrabber.com/home_help.php/form_cat_ id =2/form_sub_cat_id =9/ut=9257722ebff98f2a)
Meanwhile, Yahoo shopping will require certain number of

reviews before they can put it online. They require at least 10 reviews on the merchant in order to be able to put them in their rating and allow the merchant to use the seals on the merchants' web sites (http://help.yahoo.com/help/us/_shop/shop-71.html).

There are also seals that have problems maintaining their credibility and integrity. Some of them provide a form of certification but it cannot be verified like TechSelect on http://www.pagecomputers.com/, Sony Dealer on http://www.ssdonline.com/ and Dyson dealer on http://www.electricshop.com/. Others provide only the link to the explanation of the endorsement, which can be duplicated easily, like MasterCard Secure Code at http://www.etronics.com/ and ICRA at http://www.chumbo.com/. There are also endorsements that do not have any outside link from the original website such as Cyber Source Protected Buy at http://www.photoalley.com/. The endorsement makes self-reference to certain part of the original web site. In other words, the endorsement is endorsing its own websites.

6. Future Work and Conclusion

Based on the literature, third party endorsement has been used as one of the methods to instil consumers' trust. It enjoys a certain degree of success. Looking closely at the implementation of these third party endorsements can reveal that the merchants realize this potential since more than half of the samples have third party endorsement on their web sites. Nearly two third of those who have these endorsement are placing more than two seals to enforce their credibility and integrity of their sites. Even though there are many different type of seals available, only a few of them are being used regularly. Most of the seals are only being used on less than five websites. However, there are still many problems related to the implementation of these seals. Problems like unverifiable endorsement, misleading link, unauthorized use of logos and no endorsement at all are still there. The consumers should not take for granted the availability of the seals at the site. They need to understand the protection that being offered by the seals and the integrity level of the seals. And more research can be done in this area.

An extension of work based on from this paper is being carried out by the authors. Since finding information related to third party endorsement can distract the process of online shopping, a tool that can find and generates information related to third party endorsement will be very useful. Most of the third party endorsements are made through placement of logos on the websites and usually in the form of picture/image. Therefore, the process of identifying and extracting these logos will require an image processing technology, which is not available easily. As a solution, the current work is trying to exploit the link element of the website. The links usually contain enough information to identify which logo is being used by the websites. The same technique can also be used to navigate the page available on the whole websites. When the link is identified, the content of the page can be downloaded. The information about the

third party endorsement then in return, be evaluated and done automatically.

7. Bibliography

American Institute of Certified Public Accountants (AICPA). "Electronic Commerce assurance: Attitudes toward CPA WebTrust. Available at : http://www.aicpa.org/webtrust/yankel.htm, 1 March, 2001.

Daignault, M., Shepherd, M., Marche, S. and Watters, C., "Enabling Trust Online", In Proceedings of the International Symposium on Electronic Commerce, October 18-19 2002, North Carolina, pp 3-13.

Cheskin Research and Studio Archtype/Sapient. "eCommerce Trust Study", 1999 Available at: http://www.studioarchetype.com/cheskin /assets /images/etrust.pdf. 20 December 2000.

Cheskin Research "Trust in the Wired Americas", July 2000. Available at http://cheskin.com/p/ar.asp?mlid=7&arid=12&art=0 20 March, 2001.

Gary, G.L and Debreceny, R.. "New Assurance Service: The Electronic Frontier", **Journal of Accountancy**. (185):32-38, May 1998.

Gritzalis, S. and Gritzalis, D., "A digital seal solution for deploying trust on commercial transaction", **Information Management & Computer Security**, 9(2):71-79, 2001.

Hoffman, D.L., Novak,T.P. and Peralta, M., "Building Consumer Trust Online", **CACM**, 42(4):80-85, 1999

Kovar, S.E., Burke, K.G. and Kovar, B.R., "Consumer Responses to the CPA WebTrust™ Assurance, **Journal of Information System**, 14(1):17-36, 2000.

Lewicki, R.J., and Bunker, B. B. (1996), "Developing and maintaining trust in work relationship", in Kramer, R.M. and Tyler, T.R. (eds.), **Trust in Organization: Frontiers of Theory and Research**, Sage Publication, Thousand Oaks, CA, pp 114-139.

McCullagh, A. "The establishment of TRUST in the electronic commerce environment". Proceeding of the 1998 Information Industry Outlook Conference. Available at: http://www.acs.org.au/president/1998/past/io98/etrust.html. 1 February 2001.

Noteberg, A., Christiaanse, E., and Wallage, P. "Consumer Trust in Electronic Commerce: The Impact of Electronic Commerce Assurance on Consumers' Purchasing Likelihood and EC Risk Perception". Available at:

http://imwww.fee.uva.nl/~anna/pub.htm. 24 January 2001.

… "The Role of Trust and Assurance Services in Electronic Channels: An Exploratory Study". In Proceedings of the International Conference on Information Systems, December 1999, Charlotte, North Carolina, 1999.

Urban, G.L., Sultan, F., and Qualls, W.J. Qualls. "Placing Trust at the Center of Your Internet Strategy", **Sloan Management Review**, Fall, 2000 pp 39-48.