

The UK and EU have been quick to enact legislation relating to electronic signatures. But do they increase consumer confidence in Business to Consumer e-commerce?

Computer Law: Section B - Essay Question 4

Word-Count: 1924 (2061)

Due Date 15th May 2006

05004306

MSc Information Security & Computer Crime

This report will explore and analyse how digital signatures have increased consumer confidence in Business to Consumer e-commerce. The first part of this essay will highlight present-day statistics gathered from a previous essay on Internet Safety and will continue to examine the UK e-commerce laws that have been introduced to conform with European legislation. It will also contend that most consumers are unaware of the process and implications of digital signatures when purchasing goods online, and that the mechanics of electronic signatures are not a concern held by many consumers. The essay will then conclude that it is only when we have a greater number of users aware of the advantages of digital signatures, that we will then see an increase in consumer confidence.

The late nineties bore witness to the Internet's lowest point when the dot-com bubble¹ burst, consequently resulting in a recession where thousands of businesses folded due to rapidly increasing stock prices, no customer base, and huge annual losses. Over the next few years consumers grew more confident with the facilities provided by the Internet and this led to a steady increase in the number of users online. This 'ripple' effect has created a huge surge of electronic purchases which could mainly be attributed to the fact that we now have fifty-five percent (12.9 million) of Britain's households connected to the Internet². The same National Statistics Omnibus Survey reported that sixty-three percent of people aged 25 to 44 had bought or ordered goods, tickets or services online. As well as this mammoth increase, these users are becoming more and more aware of security threats to themselves, and more importantly, the security of the information such as credit card details they leave with online retailers (e-tailers). Deloitte's 2004 Global Security Survey³ revealed that eighty-three percent of survey respondents acknowledged that their systems had been compromised in the past year, compared to thirty-nine percent in 2003. Furthermore, forty percent of respondents whose systems were attacked said they sustained financial losses. To demonstrate the reality of these statistics, more and more businesses are converting their legacy sales systems to more leading-edge online equivalents. If a business's sales are solely Internet dependant, it then becomes a direct business concern if the Internet side of the supply chain fails due to fraudulent activity or exploitation of a known vulnerability of the system. This exact scenario occurred with

Amazon⁴ when on March 20th 2003 their site had to be shutdown for nearly an hour due to an incorrect price placed on an item of stock. The outcome of which was governed by section 9 (subsection 3) of the Electronic Commerce (EC Directive) Regulations 2002⁵ stating that a sale is subject explicitly to a websites terms and conditions. This was also the basis of Amazon's argument although it was reported by an independent law firm that if taken to court, it would be too costly for Amazon to take on each consumer separately. Having put this argument forward though, Amazon referred the users to a particularly ambiguous section within their terms stating:

“No contract will subsist between you and Amazon.co.uk for the sale by it to you of any product unless and until Amazon.co.uk accepts your order by email confirming that it has dispatched your product”

Amazon was relying on the understanding that when purchasing goods online it is implicit that you have agreed to the terms and conditions of the website.

Although not directly associated with a digital signature, the process of purchasing goods online uses technology that implements server-side digital certificates. These certificates implement a Public Key Infrastructure (PKI) utilising high levels of encryption between the consumer's computer and the server running the e-commerce application. As with a normal cheque or credit card payment you write your signature to “agree” that you are who you say you are, and that you accept to pay the merchant said amount. Digital signatures work in a similar fashion where during the online transaction your computer encrypts the information with your private key⁶. This process is well documented and understood in the computer security community as a means of protecting the integrity of information being transmitted on the Internet. By implication, after signing a document it becomes impossible to alter the content, and thus means that electronically signing a transaction makes it legally binding, and you cannot deny that you sent it⁷.

The legality of digital signatures was first defined in Section 7 of the Electronic Communications Act 2000 where it is stated that a ‘digital signature’ requires a certified

statement demonstrating that the signature has been authenticated against information supplied by the user. Section 7 of this act also makes admissible in evidence digital signatures relating specifically to the authenticity and integrity of the transaction. What makes the whole process of digital signatures confusing is that it has already been implemented into existing technology since 1996 through Secure Sockets Layer (SSL). SSL version 3 (also known as transport layer security) reached its final development after being co-developed by numerous organisations⁸, and was specifically designed to solve the Internet's primary flaw; that it could not previously provide secure communications from consumer to merchant. Presently, the process of purchasing an item online will involve the use of SSL technology, but current development means that the digital signature technology is not directly linked to the e-commerce applications. Instead, we have two discrete systems, one that deals with digital signatures during data communication, and another system that runs within this first system maintaining a correlation between the users and the goods they purchased. The certificate authentication and signing process is almost transparent to the user and only visible by indication of a "pad-lock" in the user's web browser.

So, in essence using digital signatures with SSL creates a route from A (consumer) to B (merchant) that authenticates and produces a secure channel between the two parties. However, how can A truly know who B is unless they know they are dealing with a reputable company? For example all transactions that occur between consumer and merchant only have one secure channel; the rest of the purchasing process is out of the hands of the individual as the merchant now has the relevant information to charge that individual. However it is at the merchant's discretion how it delivers this information to the bank, and how they store the details afterwards (for example, they could ignore what the Data Protection Act stipulates). Additionally with SSL, we do not actually know who we are dealing with, because the certificate could have been forged, or obtained through social engineeringⁱ. A recent case revealed that VeriSign, a popular Certificate Authority

ⁱ VeriSign issued two certificates to individuals claiming to be Microsoft by error -

<http://amug.org/~g/gerin/opinion/revocation.html>

(CA), had issued two certificates to individuals purporting to be Microsoft. To combat such issues, the UK process of ensuring the authenticity of digital signatures was enhanced in 2002 by European legislation.

The Electronic Signatures Regulations 2002⁹ specifically implements Directive 1999/93/EC of the European Parliament for digital signaturesⁱⁱ. This legislation has been passed to deal with the liability of certification authorities (also known as certification service providers). The primary goal of the legislation is to provide authentication mechanisms for determining data protection and the authenticity of the certification authorities responsible for distributing and managing digital certificates. This legislation provides consumer assurance that the certificates issued by a given CA will provide them with the facility to be authenticated on third-party e-commerce sites. It also provides a certain level of accountability on behalf of the CA stating that a consumer will be entitled to damages for any loss as a result of the CA's negligence. To enhance consumer confidence in the storage of their personal data, any CA established in the UK will be subject to stringent data protection laws requiring that the personal data¹⁰ held within a digital signature will only be useable for the purpose of signing electronic documents. That is, they may only process the data to the extent necessary for issuing a certificate¹¹.

Digital signatures provide an excellent means of ensuring that each party is authenticated but cannot provide any legal help when dealing with an unscrupulous merchant that simply takes the money without delivering the goods. The Electronic Commerce (EC Directive) Regulations 2002¹² was introduced on August 21st 2002 and transferred the provisions of the Electronic Commerce Directive (2000/31/EC)¹³ from Europe. This legislation was specifically developed to maintain consumer confidence when purchasing goods online (distance selling), and dictates that merchants must make clear all contact details, demonstrate that terms and conditions are freely available, and gives the consumer a right to cancel the order (subject to conditions). The purpose of this legislation is to provide what the EC has classified as "free movement of information

ⁱⁱ OJ No. L13, 19.1.00, p. 12

society services” which was introduced to remove barriers and increase competitiveness between member states.

We discussed that a certificate is basically a signed statement that something is true, and in a technical sense provides the facilities for creating a document that is un-forged, and that is tamperproof. As a result of the popularity of the Internet, it has been adapted for determining who wrote messages during some form of communication (e-mail, online transaction), but as previously discussed, we now have 12.9 million households connected to Internet. Out of these 12.9 million a large proportion of users will share access to a single PC with other family members. A digital signature tied specifically to one computer and user, could in fact be used by multiple users. This implies that having digital signatures could be detrimental to the confidence of consumers given that it is not possible to confirm who directly committed a transaction. This type of scenario can only be solved by implementing greater security measures during the checkout process to verify that a user is in fact who they say they are. Of course this would introduce an overhead for the merchant as they would be required to contact or possibly research the authenticity of the consumer’s personal details. This could be solved by introducing biometric technology whereby when purchasing goods the digital signature is generated from fingerprint or iris recognition techniques. This would place the consumer at the precise moment the goods were purchased, effectively completing the authentication and validation of the consumer in one process. Of course if it was that easy, the Government would have implemented this biometric technology earlier, but with all security implementations you need to consider the “trade-off” between security and cost. Presently there is no direct hardware cost involved to issue a digital signature to a consumer, but with biometrics you need specialised hardware and facilities for validating consumer’s identities.

Having a digital signature relies on the principle that you “trust” the entity that issued it to you in the first place. This trust reciprocates up a hierarchy with each Certificate Authority trusting the parent CA that granted them distribution powers, until it reaches a central “root” authority as defined by the Electronic Signatures Regulations 2002. But as

commented earlier, the consumer is unaware of the implications of using digital signatures and how they are integrated into online businesses. As a direct consequence the consumer cannot possibly be confident that their digital signature will not only protect them from fraud, but also that the process of maintaining a digital signature itself is secure. New and more robust authentication processes are needed for private users of 'home' pc; the aim would be to make each individual clearly identifiable as the person committing to a transaction. In the current environment digital signatures do not meet this need.

Bibliography

Bainbridge, D (2004, 5th Edition) *Introduction to Computer Law* [Book] Publisher: Pearson, ISBN: 0-582-47365-9

Casey, Eoghan (2004) *Computer Crime Investigation* [Book] Publisher: Elsevier, ISBN: 0-12-163103-6

Casey, Eoghan (2004, 2nd Edition) *Digital Evidence and Computer Crime* [Book] Publisher: Elsevier, ISBN: 0-12-163104-4

Kruse, Warren G. and Heiser, Jay G. (2004) *Computer Forensics, Incident Response Essentials* [Book] Publisher: Addison Wesley, ISBN: 0201707195

Maguire, M and Morgan, R and Reiner, R (2002) *The Oxford Handbook of Criminology* [Book] Publisher: Oxford University Press, ISBN: 0-19-924937-7

Rosenoer, J (1997) *CyberLaw* [Book] Publisher: Springer, ISBN: 0-387-94832-5

-
- ¹ Wikipedia (2006) *Dot-com bubble* [Online] Wikimedia. Available from: http://en.wikipedia.org/wiki/Dot-com_crash [Accessed 6th May 2006]
- ² National Statistics (July 2005) *Internet Access* [Online] National Statistics. Available from: <http://www.statistics.gov.uk/cci/nugget.asp?id=8> [Accessed 18th Dec 2005].
- ³ Deloitte (2004) *Global Security Survey* [Online] Deloitte Touche Tohmatsu. Available from: <http://www.deloitte.com/dtt/research/> [Accessed 14th Oct 2005].
- ⁴ Sturgeon, Will (2003) *Amazon.co.uk breaks iPaq news to customers but lawyers still aren't convinced* (Online) Silicon.com. Available from: <http://www.silicon.com/management/government/0,39024677,10003396,00.htm> [Accessed 9th May 2006]
- ⁵ Crown (2002) *The Electronic Commerce (EC Directive) Regulations 2002* [Online] Crown Copyright. Available from: <http://www.opsi.gov.uk/si/si2002/20022013.htm> [Accessed 8th May 2006]
- ⁶ Acca Global (2006) *What are digital signatures and SSL web server certificates?* [Online] Acca Global. Available from: http://www.accaglobal.com/members/services/digital_signatures/what_are_dig_signatures [Accessed 9th May 2006]
- ⁷ Government Gateway (2006) *More about certificates* [Online] Government Gateway. Available from: https://secure.gateway.gov.uk/Help/Help.aspx?content=help_more_about_certificates.htm&languageid=0 [Accessed 10th May 2006]
- ⁸ Wikipedia (2006) *Transport Layer Security* [Online] Mediawiki. Available from: http://en.wikipedia.org/wiki/Secure_Sockets_Layer [Accessed 8th May 2006]
- ⁹ Crown (2002) *The Electronic Signatures Regulations 2002* [Online] Crown Copyright. Available from: <http://www.opsi.gov.uk/SI/si2002/20020318.htm> [Accessed 9th May 2006]
- ¹⁰ Out-law News (2002) *Electronic Signature Regulations now in force in UK* [Online] Pinsent Masons. Available from: <http://www.out-law.com/page-2430> [Accessed 11th May 2006]
- ¹¹ Bristows (2002) *The Electronic Signatures Regulations - implications for on-line contracting* [Online] Bristows. Available from: http://www.legal500.com/devs/uk/it/ukit_100.htm [Accessed: 10th May 2006]

¹² Crown (2002) *The Electronic Commerce (EC Directive) Regulations 2002* [Online]
Crown Copyright. Available from: <http://www.opsi.gov.uk/si/si2002/20022013.htm>
[Accessed 8th May 2006]

¹³ DTI (2006) *International ICT Policy - Electronic Commerce Directive* [Online]
Crown Copyright. Available from:
<http://www.dti.gov.uk/sectors/ictpolicy/ecommsdirective/page10133.html> [Accessed 9th
May 2006]