HOW STANDARDS (SUCH AS XML) ACCOMPLISH ELECTRONIC AUTHENTICATION IN WEB SERVICES

Dana van der Merwe
Bluris LLD
Professor, University of South Africa

SUMMARY

Paper documents and "wet" signatures (made with ink) have given way to electronic data messages. This has led to problems with regard to the authentication of electronic "documents". The present article explores some solutions in the shape of standards, eXtended Markup Language (XML) as a standardised format for data and the distinction between the (modern) Protocol and (traditional) Paper points of view in this regard.

1 INTRODUCTION

According to the influential work by Toffler,[1] man has had three major eras of endeavour with three different commodities which served as a yardstick of success in each. The first wave constituted the Agricultural Revolution when one was known (and even titled) according to the land which one owned.[2] The second wave happened during the Industrial Revolution when one became famous according to the capital which one was able to invest, although the labour movement later formed an important counterpoint to the capitalists. Finally, the third wave is known as the Information Revolution, where one's success may be measured by one's access to, and control of, electronic data or information.

There seems to be little doubt that the future marketplace is going to be electronic. Not only is it going to be electronic, but the emphasis is slowly moving from e-commerce (electronic commerce) to m-commerce (mobile commerce). A few years ago I pointed out that lawyers will in future have to brush up on their computer skills, because a prerequisite to successful e-commerce will be the necessary legal and regulatory infrastructure.[3] The present article constitutes an effort to aid all lawyers in that regard.

---

1 *The Third Wave* (1980).

2 *Eg*, the Duke of Cornwall and the Earl of Leicester. Each was famous because he owned a piece of real estate.

3 Van der Merwe "Die Regsimplikasies van Elektroniese Handelsdryf ("E-Commerce") met Besondere Verwysing na die Bewysreg" 1999 *THRHR* 226ff.

Central to the understanding of this "brave new world" is a mastery of the terminology that is used. We shall therefore first take a look at the legal, technical and commercial synergy between four contemporary buzzwords. These words are "Web Services", "Service Oriented Architecture", "Electronic Signature" and "XML".

Web Services constitute the latest form of e-commerce, which is really no more than trading on the Internet[4] by electronic means. A Service Oriented Architecture provides centralised access to the discovery, use and re-use of Web Services as well as secure, federated information management. Electronic signatures form a modern part of the traditional legal world, in particular the Law of Evidence, but rely on the new standard of XML. Finally, XML stands for "eXtended Markup Language" and is closely related to HTML,[5] which is the language by means of which almost every web site on the Internet has been created.

Hopefully the attentive reader will gain some insight from the present article which might help him or her to understand "what all the fuss is about". No lawyer or businessman can really afford to remain ignorant on the above four topics. As one of the infamous James brothers said when asked why they robbed banks:

> "That's where the money is!"

Nowadays e-commerce is where the money is, at least potentially. If this new form of trading is to become successful, particularly in its latest incarnation of Web Services, the present problems with regard to on-line authentication will have to be solved. This article will argue that XML, coupled with electronic signatures, can address this outstanding issue and so engender the confidence which is needed for Web Services to really take off.

In a parallel development to "Web Services", an equally important, although less well publicized, development has been that of the "Semantic Web". This is all about new structures being imposed on data, which makes that data more accessible to human understanding and therefore more suited to human access. This aspect will also be explored under the next heading.

Finally, this article is also about the importance of standards. The presumption of regularity in the law of evidence[6] is really the inspiration behind the trust which following an accepted procedure may inspire. It would, for instance, take too much time and slow things down too much to repeat an elaborate digital signature procedure for regular transactions between regular partners, provided that those transactions adhere to a *modus operandi*[7] which has been reached by long usage or by prior agreement. Such an agreement might be on a unique procedure specific to transactions between particular parties, or it might consist in a general notice on a web-site that all transactions have to adhere to an established and well-

---

4 Also known as the "World Wide Web".

5 Hypertext Markup Language.

6 Namely that if something has been regularly done this way in the past (and nothing went wrong), we may presume that nothing will go wrong now if we follow exactly the same procedure.

7 Literally a "way of doing".

publicised procedure, or *standard*. Standards will therefore form a continuous thread in all the topics that we are going to examine.

2 WEB SERVICES, THE SEMANTIC WEB AND SOA

According to many industry observers, Web Services are going to constitute the so-called "Holy Grail" for e-commerce. They are going to succeed where the "dotcom-boom" has turned into a "dotcom-bust" and ruined so many speculators in the new economy.

Web Services have replaced[8] the existing standard and form of on-line trading, namely Electronic Data Interchange (EDI). The latter constituted a standard for the exchange of electronic documents and worked by means of requiring exactly the same format and sequence of fields to be used in such documents. EDI is only possible in a business-to-business (B2B) scenario where all contracting parties are well known to each other and have, in fact, signed a pre-contracting contract which sets out all the rules of play. EDI imposes structure on documents by counting spaces from the left side of a page and ensuring that certain fields always appear in the same position on a line. Thus the following line[9] expresses the supplier's name and address as well as some additional contact details in "EDI-speak":

"NAD SU J BLOGG INC 101 STREET BOSTON, MA 12345 US"

In the above example, "NAD" stands for "Name and Address", whereas "SU" explains the role of the data subject, namely that of "Supplier". This is then followed by the name of the supplier, namely "J Blogg Inc." and by his address in Boston. Most of the address details are self-explanatory, with "MA" representing the state of Massachusetts, "12345" the postal (or zip) code for that city and "US" representing (of course) the United States of America.

According to informed commentators,[10] one of the disadvantages of EDI has been the fact that any inherent semantic information in the data disappears after it has been transformed into the EDI format. To an uninformed reader, the expressions "NAD" and "SU" mean nothing and these have to be looked up in a separate specification document.

As will be explained later on, XML has made possible a much more sophisticated structure for e-commerce, one which will also be useful for a business-to-customer (B2C) scenario.[11] The EDI fragment above may also be rendered in XML, as will be shown under paragraph 3 below, and which example will (hopefully!) speak for itself.

---

8 Or are in the process of displacing.

9 Taken from a UN/EDIFACT example as quoted in O'Neill, Hallam-Baker, MacCann, Shema, Simon Watters and White *Web Services Security* (2003) 6.

10 O'Neill *et al* 7. See also, for a local counterpoint, the article by Eiselen "Elektroniese Dataverwisseling (EDV) en die Bewysreg" 1992 *THRHR* 204.

11 B2C is "one to many" – for instance, the Amazon.com website selling its books to any Internet user, without any prior contract or agreement on procedure.

The term "Web Services" has been defined (by IBM)[12] as follows:

> "Web Services are self-contained, modular applications that can be described, published, located, and invoked over a network, generally, the World Wide Web."[13]

It might, of course, be dangerous to define a concept simply at the hand of its transport mechanism. A "web" of functionality need not be confined to the present World Wide Web or to its underlying Hypertext Transport Protocol (HTTP). Nonetheless, the term "Web Services" has gained a life of its own and will therefore be used basically to describe modern e-commerce in this article.

In order to gain a little more perspective on this new phenomenon, another definition might be in order. The following definition comes from the book *XML Programming: Web Applications and Web Services with JSP and ASP*:[14]

> "[A] Web service is a distributed application that allows maximum interoperability between components written in different languages and running on different platforms. It is generally agreed upon that this kind of interoperability is achieved by encoding interactions between components in an XML protocol."

The authors of the last quotation also introduce and distinguish a number of XML-related acronyms which will feature again later in this article. The following three are especially important and constitute additional features to Web Services.

In the first place Web Services have "an XML-based message format called Simple Object Access Protocol (SOAP)".[15] Next comes a meta-description of its access points and interfaces in an XML-based "Web Services Description Language (WSDL)".[16] Finally, Web Services are "registered with one of several synchronized, online registries that maintain their entries in an agreed-upon, XML-based format",[17] which format is called "Universal Description, Discovery, and Invocation (UDDI)".

Put in slightly simpler terms, SOAP is the language (or protocol) in which to couch the messages which are going to deliver the Web Services. The entry and exit points (or interfaces)[18] to the Web Services are known as WSDL and this language enables an organisation to define its services in such a way[19] that a Web Service broker can formulate a SOAP message to bind to it. The registry (or library) which keeps score of all these goings-on, is known as UDDI.[20] UDDI also has an important advertising function, in that a Web Service provider may use its functionality to publish information

---

12 International Business Machines, one of the major hardware and software players in the IT industry.
13 O'Neill 4.
14 Nakhimovsky and Myers (2002) 425.
15 Nakhimovsky and Myers 426.
16 *Ibid*. The term "its" refers to Web Services.
17 *Ibid.*
18 Which might be an "http"-web address, or even the spreadsheet from which relevant data will be accessed.
19 This is analogous to putting one's address in the "telephone book".
20 Which is analagous to the "telephone book" itself.

concerning its services, so that a Web Service requester can find that particular service.

These developments take us into what has been broadly termed, "the Semantic Web". Basically semantics are all about getting to the true sense of (sometimes very obscure) subjects or objects. Even before the Semantic Web came on the scene, relational databases helped their users to new insights, simply by juxtaposing[21] certain disparate fields of data. Later on, programmers started making use of "object-oriented programming" (OOP), where each object is a separate complex of data with its own characteristics and behaviours,[22] independent of surrounding data. An object is also one instance of a class. Following upon this development, "the software industry has recently standardized a single notation called the Unified Modelling Language (UML) to model class hierarchies".[23] UML makes use of graphical representations to convey an understanding of some very complex webs of semantic relationships.

Nonetheless, relational databases, object-orientated languages and UML are all categorised as "knowledge representation"(KR) languages, which preceded the Semantic Web.[24] The so-called "Semantic Web Languages" include KR languages such as Resource Description Framework (RDF), DARPA[25] Agent Markup Language (DAML) and Ontology Inference Layer (OIL), as well as the combination of the latter two into OWL.[26] In all these references to "Ontology" it should not be seen in its philosophical sense as "a branch of metaphysics concerned with the nature and relations of being", but rather in the IT engineering sense of "a specific vocabulary used to describe [a part of] reality, plus a set of explicit assumptions regarding the intended meaning of that vocabulary".[27]

Whereas the term "Web Services" carries with it a distinct commercial connotation, "Semantic Web" is a more abstract, philosophical concept, which reminds one of artificial intelligence (AI) which was so much in vogue during the 1980s. Personally I have a feeling that the Semantic Web is likely to have much more staying power than AI, in the same sense that "Web Services" is likely to have much more staying power than the "dotcom-boom".

One of the most recent developments in this regard, which some people see as a key to the success of Web Services, is the phenomenon of "Service-Oriented Architecture"(SOA). Basically this is an architecture which acts as a library, or registry, for web services. An example is the "Sun Service Registry"[28] which supports not only Web service registry functions, but also represents a tightly integrated repository and functions for organisation, storage and control of any kind of service metadata or artifact.

---

21 Literally "putting things next to each other".
22 Also known as "methods".
23 See Daconta, Obrst and Smith *The Semantic Web* (2003) 104.
24 Daconta *et al* 217.
25 Defense (*sic*) Advanced Research Program.
26 Even though "Web Ontology Language" should really be "WOL" it is called "OWL" in honour of Owl in the children's book *Winnie the Pooh* (Milne 1996) who spells his name "WOL".
27 For a full explanation see Daconta *et al* from 185ff.
28 *Sun Service Registry for SOA Supports UDDI 3.0 and ebXML Registry 3.0 Standards* at http://xml.coverpages.org/ni2005-06-15a.html.

The Sun Service Registry is based on a number of established standards in addition to ebXML[29] Registry 3.0 and UDDI[30] 3.0. These are XACML[31] 1.0, SOAP[32] 1.1 with attachments, WSDL[33] 1.1, XML Signature1.0, XSLT[34] 1.0, Web Services Security, SOAP Message Security 1.0, WS-I[35] Basic Security Profile 1.0 and SAML[36] 2.0. Since it is implemented entirely on the Java[37] platform the Registry supports Java standards such as JAXR[38] 1.0, JAX-RPC[39] 1.1, SAAJ[40] 1.2, JAXB[41] 1.0, JAXP[42] 1.2 and SQL[43] –92.

3 XML

3 1 What is XML, exactly?

We will now have a look at what advantages XML or Extended Markup Language may bring over and above the older technologies such as EDI.[44] In particular, are there any legal advantages locked up in XML? Why do promoters of Web Services consider XML to be an indispensable part of the new scenery?

The best starting point might be to show readers an example of XML in all its naked glory. They may then compare this code with the corresponding EDI code cited under paragraph 2 above. In order to convey the same basic information as was used in that example, the XML code would read as follows:

```
<NameAndAddress Role="Supplier">
        <CompanyName>J Blogg Inc</CompanyName>
        <AddressLine>101 STREET</AddressLine>
        <AddressLine>BOSTON</AddressLine>
        <AddressLine>MA</AddressLine>
        <Zipcode>12345</Zipcode>
        <CountryCode>US</CountryCode>
</NameAndAddress>
```

[29] "e-business XML".
[30] "Universal Description, Discovery and Invocation" (in other words, how to describe something so that it may later be found again and called into use).
[31] "eXtensible Access Control Markup Language" (in other words, how to use XML to control access to the gates).
[32] "Simple Object Access Protocol" (the way to access a self-sufficient piece of data).
[33] "Web Services Description Language".
[34] "eXtensible Stylesheet Language Transformation" (how to change the way a piece of XML looks).
[35] "Web Services Interoperability".
[36] "Security Assertion Markup Language" (how to keep the bad guys out while letting the good guys in!)
[37] Java is a computer language.
[38] "Java API (Application Programming Interface) for XML Registries" (or how to get to the XML data by means of the Java programming language).
[39] "Java API for XML-based Remote Procedure Calls" (or how to invoke remote procedures by means of the Java program and XML data structures).
[40] "SOAP with Attachments API for Java" (how to handle SOAP-messages and their attachments by means of the Java language).
[41] "Java API for XML Binding".
[42] "Java API for XML Messaging".
[43] "Structured Query Language", an IBM-developed language which has become the *de facto* query language for querying databases in a client-server network.
[44] An example of EDI relating to Joe Bloggs may be found under the previous heading.

At first glance, this seems to be a much more verbose and crowded way to convey the same data as the spartan single line of EDI data did so economically. However, there are compensations. Now one no longer has to wonder what the cryptic acronyms "NAD" or "SU" are supposed to convey, because the names within the angle brackets clearly state the first to be a "Name and Address" and the second to constitute the role of "Supplier". In other words, the XML code is self-explanatory. Even though its relative verbosity might slow down transmission speeds, this can be overcome by means of data compression and other technical measures.

The data within the angle brackets are so-called meta[45]-data fields, also known as "meta-tags", which define and categorise the data between the meta-tags (called simply "tags" from here on). Note that each tag (*eg* <CompanyName>) is closed off with a second tag containing a forward slash (*eg* </CompanyName>). All data between these two tags, namely "J Blogg Inc" therefore falls within the category of "Company Name" and may be easily searched and found on the Internet by browsers and search programmes which have been instructed to look for company names. Note also that the <NameAndAddress> tag "contains" all the other data (tags as well their contents) before it is closed off by </NameAndAddress> right at the end.[46] This last feature enables the user of XML to build a hierarchy of tags which helps systematisation as well as retrieval.

The explanation in the previous paragraph should help the reader to understand a significant advantage of XML over HTML. Whereas the meta-tags in the latter language play an important role in the *display* of data on the Internet, the meta-tags in XML play an important role in the *meaning* of data on the Internet. For instance, the typical HTML tag "<bold>" would have following *display* function:

<bold>**Heading Number One: The Beginning**</bold>.

On the other hand, the tag "<NameAndAddress>" plays the semantic[47] role of giving *meaning* to the data which follows it. This is a much more powerful function, since by naming things one also gains much more control over those things.[48]

Given an understanding of the above exposition, a legally-aware reader would probably begin to see the potential of XML for law. In practice, XML has already started to play an important role in the following legal fields, one of which will be examined more fully under the heading of "XML in Evidence" below:[49]

- Law of Evidence, particularly with regard to electronic and digital signatures;

---

45 A Greek word used as an English prefix to mean "above", "beyond" or "at a higher level". In other words, "meta-data" means data at a higher level which defines and categorises the lower-level data.

46 I have used indentation to make the point even more strongly, although the authors of the work (O'Neill *et al* 6 and 7) from which the above example (as well as the EDI example) come, have not done so.

47 "Semantic" is defined by the *Concise Oxford Dictionary* (1983) as: "relating to meaning in language" and "relating to connotations of words".

48 As Adam reportedly did with the animals in Paradise.

49 For some of the other fields, see my article Van der Merwe "XML and the Law: Where the Former is Taking the Latter" 2005 *THRHR* 69.

- Intellectual Property, with regard to digital rights management, namespaces *etcetera*;
- Law of Contract, particularly when contracting online;
- Law of Privacy, particularly the sophisticated possibilities which XML offers for data protection; and
- Legal Informatics.[50]

XML also plays an important role in the field of security. Much as it galls a lawyer[51] to say this, if security can accomplish its goals with an effectiveness of a hundred per cent, the criminal law would probably "wither away" as some optimists in the Communist camp have predicted. In fact, "prevention is better than cure" and it is therefore interesting to note that XML can play a very important role in security as well as in law.

3 2 XML and security

Given that XML is likely to be the format in which data will travel in future, how secure is this new format? In fact, XML poses new and unique risks to the security procedures and installations of the participants in Web Services. The reason is that XML messages are usually wrapped in a programmed "envelope" that most firewalls can handle. These inspect the envelope but not the contents, and fraudulent XML messages may thus enter corporate networks undetected.

The above relates to "bad" XML messages getting to the "good guys". The converse is also a major problem, namely "bad guys" getting access to "good" XML messages. This may happen when hackers intercept or monitor confidential XML messages, with potentially disastrous results for both messaging parties. This activity is potentially much more damaging than simply hacking into a website, because the communications may be exposing valuable private or corporate information.

The theme of XML and Security has had two different interpretations. The reason for this is mainly because of two different visions of what Web Services should really look like.

The first is that of the Microsoft World which foresees a Microsoft Services (MS) World in which all programmers will do their thing in Visual Basic or C++ (both languages being owned by MS, incidentally), using the latest Windows operating system (also owned by MS), to whom Java is simply a large island in Asia, somewhere.[52] Nonetheless, XML plays a very important role in this vision and the latest MS Web Services-strategy, DotNET, is very much based on XML. Their 2003 XML Office package has also integrated XML nicely into packages such MS Word, MS Excel, MS Outlook, *etcetera*. In order to look after security concerns in DotNET, MS has designed their so-called "Passport technology". The main goal of the latter technology is to provide a single sign-on implementation that will provide trusted interaction

[50] Strictly speaking the last field is not about the law solving IT-related problems, but about IT helping the law to function better. See Van der Merwe *Computers and the Law* (2000) 265ff.

[51] The present author being a lawyer by training, profession and inclination.

[52] In fact, MS has licensed Java from Sun Microsystems, only to fashion their own flavour of Java called "J++".

between participants, because everyone would have been authenticated before being able to get on to the system.

The alternative vision is that of Java geeks[53] programming in "their" language, using Linux or some other open source operating system. The Java programming language has also very much become "XML-aware", as such acronyms as "Java Architecture for XML Binding" (JAXB), "Java API[54] for XML Messaging" (JAXM), "Java API for XML Processing" (JAXP), "Java API for XML Registries" (JAXR) and "Java API for XML-Based RPC" (JAX-RPC)[55] illustrate.

Sun Microsystems, having invented Java, has also initiated the so-called "Liberty Alliance Project".[56] This project has now been joined by considerable numbers of other important players in the industry. Its main goal is to enable a single sign-on for each member in order to communicate with trusted correspondents. This involves creating so-called "Circles of Trust" among identity providers and service providers which will lead to trust relationships backed up by legal agreements.

Due to the differing portfolios of intellectual property at stake, it appeared as if the two protagonist firms were heading for a show-down in the copyright courts. Fortunately, due to an historic agreement between Microsoft and Sun in April 2004, it seems that the two visions described above might be merged after all, with XML being a strong connecting link in the final product.

A strong security technology in any future Web Services development is likely to be SAML.[57] This has been developed by OASIS[58] and has reached the status of an "OASIS Open Standard". This language enables trust assertions to be specified using XML, which assertions may relate to authorisations, authentications and attributes of specific entities, whether these are individuals, legal persons or computer systems.[59] These digital assertions are now rapidly taking the place of traditional documentary guarantees of authenticity and trust. The matter will be discussed under paragraph 4 below which deals with the law of evidence.

The trust assertions mentioned in the previous paragraph refer to the so-called "building blocks of security".[60] These are constituted by the following: authentication, integrity, nonrepudiation, privacy and availability. Although these are all security concepts, the first three are also accomplished legally by means of a signature, and in the digital world of Web Services, by means of a digital signature. This subject will again be treated in greater detail under paragraph 4 below.

---

53 Slang expression for a technically obsessed person who spends so much time with the computer that other dimensions of personality (such as social skills) are poorly developed. This definition and some of the following, come from *Webster's New World Dictionary of Computer Terms* (8ed).

54 Application Program Interface. In Web servers, this means the standards or conventions that enable a hyperlink to originate a call to a program that is external to the server.

55 Remote Procedure Call. A protocol that enables one program to request another program, located elsewhere on the network, to execute or supply certain data.

56 See http://www.projectliberty.org/ for further detail in this regard.

57 Secure Assertion Markup Language.

58 Organisation for the Advancement of Structured Information Standards.

59 For more detail on the fascinating topic of SAML readers may consult the work of O'Neill *et al* 102ff, cited earlier on.

60 O'Neill *et al* 22ff.

Before dealing with the legal way in which to accomplish the five goals mentioned above, we have to mention that one may also attempt to reach the same goals by means of security measures.[61] The main security technology in this regard, is that of encryption. Up to now "Secure Sockets Layer" (SSL) has been very successful in accomplishing a reasonable level of security in e-commerce. This is a security standard that is widely supported among Internet browsers and servers and which is thus platform-independent. It is also application independent because it works at the network layer rather than at the application layer. Applications that use SSL also use RSA[62] encryption and RSA public certificates and digital signatures.[63]

Two mechanisms by means of which security may be practically implemented are smartcards and biometrics. A "smartcard" refers to any creditcard-sized device that contains a microchip (or processor).[64] This works very effectively while it remains in the hands of the lawful owner or possessor, but once it (literally) falls into the wrong hands, it may turn into a double-edged sword. It produces an almost perfect misrepresentation to the poor computer or ATM which is supposed to "identify" the person interacting with it.

In this regard, biometrics might be a better and more permanent solution. Because the fingerprint[65] of each individual is unique, it might be more prudent to substitute the smartcard-reader with a fingerprint scanner. The iris of the human eye is also unique, and the banking client might therefore simply be required to "peep into the keyhole, please"!

Biometric identification has been defined as follows:

> "It is a form of electronic signature which entails a quality linked or attributed to the person of the user, such as fingerprints and retinal structures, within the electronic environment, which is known as biometrics"[66]

and as

> "(T)he science that involves the statistical analysis of biological characteristics".[67]

Apparently these characteristics may include *physiological*-based techniques such as facial analysis, fingerprinting, hand geometry, retinal and iris analysis and DNA profiling. In addition one finds the *behavioural*-based techniques such as signature, keystroke, voice, smell and even sweat-pore analysis![68]

In South Africa, the Department of Home Affairs has announced its intention to go the biometric electronic passport route from 2007, making it

---

61 Remember once again the old aphorism, "Prevention is better than cure".
62 The acronym "RSA" comes from the names of the three inventors of the algorithm used for this type of encryption, namely Rivest, Shamir and Adleman.
63 The question of certificates and signatures will be covered under par 4 below.
64 See O'Neill *et al* 33ff.
65 Or palm-print, or footprint.
66 Robinson *The Development and Application of the Signature as an Identification Method in South African Law* (unpublished LLM dissertation Vista University, 2002) 61.
67 Robinson 62.
68 *Ibid*.

the first country in Africa to do so.[69] Standards play a role again, as the new passports will have to comply with the minimum e-passport requirements as defined by the international ICAO[70] 9303 specification. The passports will also contain an embedded contactless[71] "smart-card" chip that will digitally store South Africans' biographic data, digital photos and other information.

Even in the area of biometrics XML has started to play an important role. The XML Common Biometric Format Technical Committee is planning to take several existing biometric standards and develop versions of them that are based on Extensible Markup Language.[72] According to Griffin, chairman of the OASIS committee in this regard, their activities have the following goal:

> "The goal is to bring industry to some framework for expressing biometric information so that they could eventually eliminate all the proprietary formats that prohibit different biometric solutions from being able to be used together."

The XML Common Biometric Format (XCBF) is the latest in a series of efforts to address the above problem. More significantly, it is the first format for biometric standards to be based on XML. The problem with previous standards was that these were in binary[73] format, which could not interact with XML systems and applications. One requirement for the success of the new standard would be adoption by powerful players in the industry and Griffin argues that government and other large customers should start playing a more important role in this regard.

To conclude this part on XML and security, it seems that the only hope for secure Web Services in future would be for security professionals to familiarise themselves with this new language and all its ramifications. For example, security experts should learn more about how to validate Web Services Description Language (WSDL), the protocol that describes what a given XML application does.[74] In addition, they should make full use of the existing security techniques, such as Secure Sockets Layer (SSL)[75] to get all the protection they can.[76]

3 3 XML and standards

The United States has become an eager disciple of XML, especially after the unfortunate events of 11 September 2001.[77] Their Department of Justice has turned to XML to assist them in their time of need for quick, yet reliable,

---

69 "SA's e-passport to debut in 2007" (2005-07-14) *iWeek* 6.

70 International Civil Aviation Organisation.

71 Conforming to the standard of the International Standards Organisation (ISO 14443).

72 "XML biometric standards jell" at the Federal Computer Week website (FCWCOM) published on the web at www.fcw.com (5 July 2002).

73 A system made up by the two (therefore "bi"-nary) digits "1" and "0". The latter represent the "on" and "off" states of an electrical system. The opposite to binary files are ASCII files which are made of readable letters and numbers.

74 See above, par 2 on Web Services in general.

75 See the discussion of SSL higher up in this section.

76 See further LaMonica "Extra Headaches of Securing XML" visited http://news.com.com/2102-7345_3-5180510.html (5 May 2004).

77 See Van der Merwe 2005 *THRHR* 69 for more details in this regard and on the criminal law in general.

data. Thus a "Justice Information Exchange Model" (JIEM) as well as a "Justice XML Data Directory" (JXDD) has been developed.

The different federal states have also been active in the area of justice and XML. To mention but one example, the Georgia Tech Research Institute (GTRI) has created a "Justice XML Information Center" and its "Global Justice XML Data Model" (GJXDM) and "Global Justice XML Data Dictionary" (GJXDD) have been adopted by almost all the other federal states.

Mention has already been made under the previous heading of the huge growth of XML in the securities industry. That industry is also in great need of standards, for the reasons set out in the final paragraph of paragraph 1 above. A brief history in this regard[78] might be informative.

In the 1970s the financial industry created the SWIFT-standard for global processing of the data and documents attendant upon the trading of securities. In the 1980s, ISO[79] defined the standard ISO 7775 which was deployed on SWIFT during the years 1984 to 1997. From 1994 to 1999 ISO defined a new standard, ISO 15022, which was implemented in 1999. ISO 15022 serves as a high level description of the modeling[80] approach to the financial industry; as a high level description of a "Repository" (for standards); for the definition of registration bodies as well as for service level agreeements.

The relevance of this history becomes apparent when one takes notice of the activities of working group (WG) 10 of ISO 15022. Their mission statement is the following:

> "Evolve ISO 15022 to permit migration of the securities industry to a standardized (*sic*) use of XML, guaranteeing interoperability across the industry and with other industry sectors, particularly but not restricted to the financial industry."

The WG is to take into account international initiatives on message standards such as ebXML.[81] The use of XML is supposed to offer "stability" (XML is a permanent standard); "interoperability" (end-to-end communication based on common semantics); "flexibility" (using the excellent categorisation which XML offers to represent asset classes, for instance); as well as "predictability and speed" (XML fosters reuse and automation capabilities). XML is also likely to be useful for evolving existing standards and creating new standards, as well as for a standards repository.

In addition to the above, SWIFT has published *SWIFTStandards XML for Implementors*[82] as an

> "[I]mplementation manual for SWIFTStandards XML messages. It complements the SWIFTStandards Reference Guide and the SWIFTNet Developer's Toolkit."

---

78 From *ISO 15022 XML: A Model for Standards Convergence*, a presentation by S Dinetz at the Depository Trust and Clearing Corporation (DTCC) Interoperability Summit held on 27 June 2002.

79 International Standards Organisation.

80 Obviously the Unified Modelling Language (UML) also plays an important part.

81 E-business XML.

82 Published during January 2004.

All standards concepts are also given with their UML modeling representation equivalents.

To summarise, SWIFT expects full conversion to XML to take up to 10 years and "to be driven by users' willingness to tap new revenues and expand their businesses".[83] On the other hand, XML is likely to shorten the time of deployment of standards significantly and also to make subequent maintenance "a lot easier".[84]

4 ELECTRONIC SIGNATURES AND XML

4 1 Introduction

Before starting upon what is really the *heart* of the present article, I must first endeavour to challenge the *minds* of readers who have made it thus far. Most people think of the area of documentary evidence, of which traditional signatures very much forms a part, as being related to paper. Paper is signed, the original document has to be stored (in some file) for possible future forensic use, the integrity of the document can be physically checked by examining it for erasures, the age of the ink, the physical pressure of pen upon paper, *etcetera*.

The problem is, of course, that almost nobody sits down to write with a pen on paper anymore. Almost all "documents" (whether created privately or for business purposes) are electronic ones, being created within the belly of the beast (the computer) by energetic typing on its keyboard. If the document is likely to be important in future, we sign one print-out[85] by means of a "wet" signature (in other words, by means of pen and ink). This creates one "original" from among thousands of potential copies. This reduction of a digital document to a corporeal one for evidential purposes was the model for South Africa's first foray into computer legislation, namely the Computer Evidence Act[86], which will be discussed under paragraph 4 2 below.

An entirely new perspective might be to distinguish between the "paper" and "protocol" points of view, when dealing with documentary evidence that originates from a computer or other digital device.[87] This distinction has been made in Appendix E of the work *Secure XML*[88] and will be set out in the following number of quotations. Let us then first have a look at the above authors' view of the evidential implications arising from a computerised version of paper documents (the "paper" protocol):

> "PAPER: The important objects are complete digital documents, analogous to pieces of paper, viewed in isolation by people.
>
> A major concern is to be able to present such objects as directly as possible to a court or other third party. Because what is presented to the person is all that is important, anything that can affect it, such as a style sheet, must be

---

83 *Migration to XML Standards Will Be Slow, Not Swift* by M DeWeirdt, head of standards at SWIFT, at http://www.financeasia.com/articles/1982BB53.

84 *Ibid*.

85 Known as a "hard copy" because it now exists in physical format (a piece of paper).

86 57 of 1983.

87 Nowadays, messages sent from, or stored on, cell phones or other digital devices such as the "Palm", "I-Paq" and "I-Pod" might also become relevant in court.

88 Eastlake and Niles (2003) 469.

> considered an intrinsic part of the paper. Sometimes proponents of the paper orientation forget that the 'paper' originates in a computer, may travel over, be processed in, and stored in computer systems; and is viewed on a computer. Such (*sic*) operations may involve transcoding, enveloping, composition of messages from pieces of other messages, or data reconstruction."[89]

In other words, if parties really want to show the required "original document" to a court in digital format, counsel should bring his (or her) laptop computer to court and the court should be technically astute enough to check the underlying style sheets, word processing programme, (smart) card reading devices and other peripherals for their influence on what is being shown on screen. Making a printout of the above only creates an illusion of immobility, unless the printout is signed and dated by means of a wet signature, which takes it out of the realm of digital signatures anyway.

Let us now have a look at the authors' view of the legal implications from a "protocol" point of view:

> "PROTOCOL: What is important are bits on the wire generated and consumed by computer protocol processes. The bits are marshaled into composite messages that can have rich multilevel structure. No person ever sees the full message as such; rather, it is viewed as a whole only by a 'geek'[90] when debugging – even then he or she sees some translated visible form. If you ever have to demonstrate something about such a message in a court or to a third party, there isn't any way to avoid having experts interpret it. Sometimes proponents of the protocol orientation forget that pieces of such messages are actually included in or influence data displayed to a person."[91]

According to this point of view, we no longer have counsel nervously handing up his laptop computer to the presiding officer in order to "produce" a document before the court. To the relief of the judge[92] he (or she) now gets a neatly typed transcript and simply has to evaluate the testimony of the technical expert who has to explain why the contents of the transcript may be trusted despite its journey through the bellies of several computers and other devices. Documentary evidence is thus allied with another area in the field of the law of evidence, namely expert evidence. It is also clear that, at least according to this philosophy, we should stop thinking about paper documents and signatures and start comprehending protocols, canonicalisation and other strange and wonderful words. These terms all really boil down to generally agreed-upon standards which have to be followed if a document is to have any evidential weight in court.

The authors take a whole chapter[93] in order to deal with the concept of "XML canonicalization: the Key to Robustness". They define the phrase "canonicalisation" as follows:

> "It is the extraction of the 'standard form' of some data and the discarding of 'insignificant' aspects of the data's surface representations, usually by restricting all surface representation choices to a single option."

---

89 Eastlake and Niles 470.

90 See the definition of "geek" in fn 53 above.

91 Eastlake and Niles 470.

92 Older people are usually technologically challenged! A notable exception to this rule being Chris Schmidt, emeritus professor of Unisa and the author of several editions of his authoritative handbook on Evidence. He was already using MS Word while the rest of us were still on IBM Display-write!

93 Eastlake and Niles 169ff (Chapter 9).

As we shall see, canonicalisation together with encryption and XML itself are all necessary ingredients in order to create an XML digital signature. The latter is likely to prove the only reliable way to "sign" documents as part of Web Services or in any other form of e-commerce.

The problem is that even simple text, when sent from one computer application to another, might undergo a number of changes. These may consist of a change in line-ending characters, removing or adding spaces at the ends of lines, tab characters may have been converted into spaces, etc. Even namespaces present problems because of the location-specific and relative way of referring to these. Even though these changes seem insignificant and not really legally relevant according to the "paper" point of view, they also mean that the total number of bits and bytes might have changed and that the document is no longer the same in terms of the "protocol" point of view. This disparity is highly significant because digital signatures (as well as encryption) can only work by adding up the number of bits actually received and checking them against the number mentioned in the "envelope" that was sent off, before subjecting these bits to further electronic operations.

It seems that the Xpath data model will be used in future as the standard for the canonicalisation of XML data. That is because this model retains namespace prefixes in exactly the same format and can handle the "Enveloped Signature Transform"[94] model quite well.

4 2 The Computer Evidence Act 57 of 1983

This Act was a sort of emergency measure by the South African Government, after the case of *Narlis v South African Bank of Athens*[95] rather cruelly exposed the inability of the South African law of evidence to handle documents that had been stored on computer.

In this case the bank was trying to submit in evidence extracted from its computerised records and tried to make use of section 34 of the Civil Proceedings and Evidence Act[96] which deals with the admissibility of documentary evidence as to facts in issue. The section uses the phrase "person who made the statement" once or twice, which led to the following (rather triumphant) remark from Holmes JA:

> " Well, a computer, perhaps fortunately, is not a person."

As a result the evidence was held to be not admissible. The Clearing Banks Association immediately instructed a judge[97] to prepare both a report on the matter[98] as well as draft legislation to cure this defect in the law. The legislation was passed one year after the report had been published (and after the SA Law Commission had also been involved) in the shape of the Computer Evidence Act, 57 of 1983.

---

94 See par 4 4 "XML Digital Signatures" below for further detail.
95 1976 2 SA 573 (A).
96 25 of 1965.
97 Justice JM Didcott.
98 Report on the Admissibility in Civil Proceedings of Evidence Generated by Computers.

The biggest criticism of this Act[99] is the fact that it still uses the paper metaphor throughout. Almost all of its provisions deal with paper documents, either in the form of statutorily defined "computer print-outs" or "authenticating affidavits". Armed with the latter, a judge needed to have no qualms in accepting the former into evidence. The deponent to the authenticating affidavit needed to have distinguished qualifications. He (or she) had to be:

> "[S]ome person who is qualified to give the testimony by reason of –
> (a) his (sic) knowledge and experience of computers and of the particular system by which the computer in operation was operated at all times; and
> (b) his (sic) examination of all relevant records and facts which are to be had concerning the operation of the computer and the data and instructions supplied to it."

This legislation was subjected to a torrent of academic criticism, even by the present author.[100] Still, one has to admit that the Computer Evidence Act at least brought forward the concept of an expert, which idea is now again finding favour. The problem with that Act, of course, is that the "expert" would obviously have been working for the company seeking to put in the records, and would therefore hardly be a disinterested witness. The "expertise" with regard to the computer and its operating system was also not defined in any objective manner.

Another section of the Computer Evidence Act foreshadowed, in my opinion, an even more "modern" and useful concept. Thus, section 2 (6) stated the following:

> "Subsections (3), (4) and (5)[101] do not apply to an authenticating affidavit which –
> (a) relates to a computer print-out of a public institution produced in the ordinary and regular course of the public institution's business or activities from data and instructions supplied to the computer in the ordinary and regular course of such business or activities; and
> (b) is deposed to by an official or employee of the public institution who is qualified to and does certify that the computer print-out was so produced."

Except for the remarkable trust which this sub-section placed in public institutions, it was also remarkable for the test of "ordinary and regular course of business" which it emphasised. The latter had overtones of the concept of canonicalization discussed above, and this aspect actually formed part of the next, improved legislative measure.[102]

4 3 The ECT Act 25 of 2002

South Africa has since adopted its own Act on Electronic Communications and Transactions ("the ECT Act"[103]) which defines the concept of an "electronic signature" in section one of the Act:

---

[99] Which was only mentioned in one reported case, as far as the present author is aware.
[100] Van der Merwe "Documentary Evidence (With Specific Reference to Hearsay)" 1994 *Obiter* 64 80ff.
[101] All of them imposing onerous obligations.
[102] The Computer Evidence Act was repealed by the ECT Act, discussed under the next heading.
[103] 25 of 2002.

> "'Electronic signature' means data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature."

The Act goes further and also defines an "advanced electronic signature" (also in section one of the Act):

> "'Advanced electronic signature' means an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37."

The "Authority" referred to turns out to be an "Accreditation Authority", because section 37 of the ECT Act informs us that "the Accreditation Authority may accredit authentication products and services in support of advanced electronic signatures".

Section 38 sets out the criteria to be used by said Authority in accrediting an electronic signature.[104] Said Authority has to be satisfied that such an electronic signature:

> "a. is uniquely linked to the user;
> b. is capable of identifying that user;
> c. is created using means that can be maintained under the sole control of the user;
> d. will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable;
> e. is based on the face-to-face identification of the user."

For purposes of accreditation, the Accreditation Authority may also have regard to various other factors relating to the authentication service provider that will provide the mechanism for performing the electronic signature referred to above. These factors relate to financial and human resources, the quality of its hardware and software systems, its processing procedures or services, the availability of information to third parties who will be relying on the authentication product, and the audits by an independent body.

In line with the protocol versus paper argument introduced under section 1 above, it is interesting to note that the object to be authenticated by means of an electronic signature is known as a "data message".

Section 1 of the ECT Act defines this concept as follows:

> "'[D]ata message' means data generated, sent, received or stored by electronic means and includes –
> (a) voice, where the voice is used in an automated transaction; and
> (b) a stored record."

Thus an electronic data document has now taken the place of the print-outs and paper affidavits of the Computer Evidence Act discussed under the previous heading.

In line with the canonicalisation arguments made above, it is interesting to note that the ECT Act also[105] contains a section which relies on the

[104] So that it may become an "advanced" electronic signature, of course.
[105] Compare the corresponding provision in the Computer Evidence Act under par 4 2 above.

presumption of regularity which flows from normality. Section 15 of the ECT Act deals with the evidential admissibility and weight of data messages in general. Section 15 (4) specifically states as follows:

> "A data message made by a person in the ordinary course of business, or a copy or a printout or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract."

This reminds one of the regular and ordinary course of business (of a public institution) mentioned under par 4 2 above, when dealing with the Computer Evidence Act.[106] Again this reminds one also of the concept of canonicalisation and how general agreement about criteria and standards helps the admissibility of documentary evidence. The problem with any really new development (such as XML) is, of course, that no such agreement exists historically. In this type of case, agreement has to be reached up front between participants in a scheme of trust and/or communication as to what mutual protocol they are going to use in future. Hopefully the development of standards in this regard will help to ease adoption by all role-players.

4 4 XML and Digital Signatures

As has been pointed out above, the ECT Act works with the broader concept of "electronic signatures". Even though a digital signature can obviously only be created by electronic means, it has gained the special meaning of a signature where the use of a private key is involved, and is defined as such in the recently-published work *Electronic Signatures Law and Regulation*.[107]

According to the author of this book (Brazell), the complexity introduced by a public and private key infrastructure bestows certain unique qualities on a digital signature. The "signed" message cannot be opened without the correct corresponding key and if it has been changed or interfered with, the two message digests will no longer match. A digital signature may thus be used to check message integrity. A drawback to the key infrastructure is that a key may be lost or compromised and the system of announcing compromised cards to the unsuspecting public is not yet working adequately.[108] Another problem is the lack of technical standardisation between the many cryptographical products on the market. This is where our old friend canonicalisation comes in again and where XML may be the solution. Unfortunately Brazell does not even mention the possibilities of XML when she laments:

> "[I]t is unfortunate that there are as yet very few truly international standards applicable to the electronic signature infrastructure".[109]

---

[106] 27 of 1983.
[107] Brazell (2004) 52.
[108] Not only because of inadequate publication, but also because most participants in Web Services just cannot be bothered to check the key revocation lists.
[109] Brazell 256.

An XML signature is simply a digital signature expressed in XML.[110] In contrast to the existing PKCS#7[111] binary[112] system which uses ASN.1[113] syntax and the PGP[114] binary system which uses its own syntax, XML signatures have their own, human-readable, syntax. The key characteristic of XML Digital Signatures (XMLDSIG) is that the signature object itself appears in XML syntax. All these digital signatures perform the function of providing integrity for the "signed" data and when linked with the signer's identity by means of an X 509-certificate,[115] may also provide non-repudiation and authentication (the "building blocks" mentioned under the security section above).

What are the advantages of XMLDSIG above other digital signatures? Because XML stratifies[116] data into layers, an XMLDSIG may be used to sign some parts of the document, for instance, those parts that are not likely to be changed any further during the course of transmission. The XMLDSIG may also be used to sign a data field contained within itself, to sign surrounding data or to sign data which is quite disjointed and separate from itself.[117] In the latter case it can sign anything that can be referenced by means of a URI and:

> "(e)ven more flexibly, they can sign anything you can derive with an algorithmic transformation from data that the URI references!"[118]

Finally, but not least important, an XMLDSIG is human-readable, and therefore also (hopefully!), human-understandable.

It might be best to illustrate the "readability" factor of an XMLDSIG by means of another real live example of XML code:[119]

```
<Signature>
        <SignedInfo>
                (CanonicalisationMethod)
                (SignatureMethod)
                <Reference>
                        (DigestMethod)
                        (DigestValue)
                </Reference>
        </SignedInfo>
        (SignatureValue)
</Signature>
```

In the above example it is clear that everything else is contained within the <Signature> element. The <SignedInfo> element contains both the procedures as well as a <Reference> to a digest of the data which needs be signed in the first place.

---

110 See O'Neill *et al* 65.
111 Public Key Cryptography System version 7, developed by RSA security.
112 This "binary blob" is not readable by the human eye.
113 Abstract Syntax Notation 1.
114 Pretty Good Privacy.
115 X 509 is an international standard for digital certificates that maintains strong authentication. The latest, version 3, also helps interoperability between software using certificates.
116 Puts the data into separate layers, according to its meaning or characteristics.
117 See the explanation of "enveloped", "enveloping" and "detached" signatures below.
118 See Eastlake and Niles 209.
119 Taken from the same work (Eastlake and Niles 214) – see also the previous example of XML-code under par 3 above.

Mention has already been made above of "enveloping", "enveloped" and "detached" signatures above. XMLDSIG may be classified according to its relationship with the data being signed as follows:

(a) An *enveloping* signature (the signed data is contained within the XMLDSIG-element;

(b) An *enveloped* signature (the signed document surrounds the XMLDSIG-element;

(c) A *detached* signature (the signed data is[120] quite separate from the XMLDSIG-element, but the latter refers to it).

Because XMLDSIG elements can sign multiple pieces of data, they can be any two or three of these kinds of signatures at the same time![121]

It seems clear that a XMLDSIG has many advantages. These are offset by the fact that XMLDSIG-code is "fat" because of its verbosity, the very factor that makes it human-readable. This disadvantage is offset, in my opinion however, by the fact that data compression is very effective nowadays, as is the speed of most modern data-processing devices.

5 CONCLUSION

It should be clear from the amount of attention which I have given to the protocol and paper points of view[122] that I consider this to be one of the keys to a solution for successful Web Services. In my view, the common law has developed in a paper-based world, never having the chance to grasp the new world that the computer was going to bring in its wake. Unfortunately, even our law-makers often act in a "BC"-fashion.[123] Even though the paper point of view might make for a more familiar mind model to think of a merchant "signing" an electronic "document" with his private key, the reality is far enough from this illusion to cause legal problems further on. Not only legal problems, but also economic ones, because Web Services need to have a firm legal infrastructure before their obvious potential can be fully exploited.

It should also be clear from the even greater amount of attention which I have given to XML, and specifically XMLDSIG, that I consider it to be part of the solution to the above problem. For the reasons mentioned above, such as the stratification of data and the human readability which XML brings with it, but especially because of the number of standards which it has spawned, I think that XML is the common ground on which the business world should unite. The protocol point of view depends on an up-front agreement about the conditions under which communications and transactions are going to follow. It shifts any uncertainty away from the moment of the specific transaction, back to the general agreement which is supposed to cover all situations. The law of evidence is likely to yield ground to the law of contract as the legal field which is going to cover electronic and especially, digital signatures.

---

[120] Because of the inherent characteristics of XML.
[121] Eastlake and Niles 210.
[122] See the Introduction to par 4 above.
[123] For purposes of this article only, "BC" represents "before computer".

The protocol world is also very dependent on universally accepted standards, especially in the area of XMLDSIG. In this regard the Electronic Signature Directive in Europe has spawned some interesting results. The European Electronic Signature Standardisation Initiative (EESSI), the European Committee for Standardisation (CEN) and the European Telecommunication Standardisation Institute (ETSI) have been doing sterling work. In the area of XML, ETSI has developed a technical report on "XML Format for Signature Policies"[124] as well as a technical specification for "XML Advanced Electronic Signatures" (XAdES).[125] The former document does not only deal with XML but also with associated concepts such as RDF and P3P. An Electronic Signature Committee overviews these developments and is due to publish a report on activities within the foreseeable future. The use of XML in the wider area of law is sponsored by an action group called LEXML.[126]

A number of specific country initiatives also exist. Thus the "Danish National XML Committee" plans to make use of UBL[127] to establish a standard for e-commerce in the public sector. In Sweden, the "Swedish Legal Information Standards Network"[128] has established an action plan focusing on three assumptions:

1 Information standards need to be legally managed;

2 The digital network society requires proactive law; and

3 Trust enhancement is the goal.

It seems that these views lean much more towards the protocol point of view than to the paper point of view.

Outside of Europe, UNCITRAL[129] has also been trying to put forward standards in this field, hoping to gain universal (or at least wider) acceptance between countries. One of the standards, outside of XML, which seems to present a bridge for better communication is the X.509-standard which has already been mentioned above. The "ISO[130]-RTU Recommendation X.509" has been described by Brazell as "perhaps the most fundamental of the electronic signature standards".[131]

In the area of XML the "LegalXML"[132] activist group acts as a prophet for the use of XML in law in general.

South Africa's ECT Act[133] has taken a step in the protocol direction with its emphasis on a "data message", rather than the paper-based view of the Computer Evidence Act,[134] which focused solely on print-outs and identifying affidavits. Unfortunately there is no mention of XML in either document, nor

[124] ETSI TR 102 038.
[125] ETSI TS 101 903
[126] See the website at www.lexml.de for instance.
[127] Universal Business Language – which builds on XML.
[128] LISA.
[129] United Nations Commission on International Trade Law.
[130] ISO is NOT an acronym for "International Standards Organisation" as is commonly thought, but derives from the Greek work *iso* which means "equal".
[131] Brazell 261.
[132] See www.legalxml.org.
[133] 25 of 1970.
[134] 57 of 1983.

in the draft regulations which have been drafted in terms of the ECT Act. Nonetheless both Acts saw value in the regularity of respectively government and business routine, as has been pointed out above when dealing with each Act. This exception to the hearsay rule for certain documents originates from British legislation such as the Police and Criminal Evidence Act[135] and the Criminal Justice Act.[136] Tapper sums up the relationship between the Acts nicely when he compares the latter with the former as follows:

> "This provision reverts to the categorisation of admissibility in this area by reference to business rather than duty."[137]

In the same way, one might mention, the South African ECT Act and Computer Evidence Act respectively focus on business and duty as guarantees of reliability. In hindsight, one might also see this emphasis on regularity as a common-law form of canonicalisation and protocol. Businessmen and government servants have, by force of habit rather than by legislation, managed to agree on some standard of behaviour which puts that behaviour on a higher standard of trustworthiness. Nonetheless, it might be better, especially in the international context, if this (unspoken) standard can be updated by means of legislation, especially if the standard turns out to be based on XML.

All in all the protocol point of view seems to be gaining world-wide acceptance, slowly but surely. In its search for generally accepted standards, also expressed as a "canonicalisation" of certain standards, XML seems to be playing a central role. XML Digital Signatures (XMLDSIG) are likely to be a crucial factor for Web Services to gain universal trust and become a commercial success world-wide.

My sincere thanks go to the readers who have followed me thus far, and I herewith tender my apologies to them for writing the legal article which probably holds the record for having used the most acronyms. Hopefully this use of acronyms has helped the author to strive for attainment of the KISS-principle[138] and not to bore his readers overmuch!

---

[135] (UK) Police and Criminal Evidence Act, 1984.
[136] (UK) Criminal Justice Act, 1988.
[137] Tapper *Cross & Tapper on Evidence* 9ed (1999) 586.
[138] Keep it short, stupid!