XML as a tool for legal validity in a security context

Cecilia Magnusson Sjöberg
Swedish Law & Informatics Research Institute
cecilia.magnussonsjoberg@juridicum.su.se

1 Purpose

The title of this paper "XML as a tool for legal validity in a security context" may in itself be regarded as a content heavy expression that may be object for an analysis resulting in marked up elements and attributes. A supporter of standardised markup languages is thus expected to take a dynamic approach to text, while those not yet knowledgable of the potentials of XML might be stuck in thinking of flat representations of key words attached to the beginning of a document or search words inserted in an (inverted) index file.

So far so good, but is the XML approach secure, and why would it be a worthwhile task to investigate in terms of legal implications? The purpose of this paper is to convey a strategy for answering that question. In more precise terms, the aim is not merely to cure curiosity but to let the attempt serve more practical interests. A legally founded checklist of XML related security-enhancing factors is namely meant to enhance the rule of law and thus promote trust in system design based on XML solutions.

The starting point is that modern document management requires coordination in order to meet demands for efficient production, supply and use. Apart from the general needs to improve recall and precision when retrieving information, there is also reason to consider, for instance, knowledge management attempts and exchange of business data in networks of various kinds.

XML has the potential to function as a lever and a sound basis for all of these developments in a modern information society. In this context, it should be mentioned that XML has a profound impact also on substantive law itself, particularly in the fields of contract law, intellectual property rights, and privacy protection. For instance, XML-messaging quite often comprises personal data processing in a legal sense (see the EC Data Protection Directive, 95/46/EC). It concerns requirements of consent from data subjects to collect, store and disseminate personal data. Furthermore, modern e-business models make it necessary to consider information duties, e.g. that the identity of a service provider must be clarified according to the EC Directive on E-commerce (2000/31/EC). Liability issues are also relevant in terms of analyzing who is responsible for the damages emerging as a result of the abuse of a transferred authentication.

As indicated above, it all boils down to trust in global digital information and a need for legal information security in open as well as closed computer based networks. Every organisation, be it a private enterprise or a public authority, needs to reflect upon the handling of documents that govern internal as well as external actions. To the extent XML may support message authentication and electronic measures to prevent distortion of (document) content is one example of an issue of extreme importance. The concept of authority covers a wide variety of actions, e.g. authorizations to enter into a contract and law enforcement.

Bearing in mind the initially mentioned checklist approach to be captured in this paper, the group of addressees or - "who will benefit" - may be described in the following way. To begin with, secure use of XML is, of course, relevant for commercial actors as well as for representatives in the public sector. To exemplify, mention can be made of buyers that in a procurement situation are dependent on a clarification of legal conditions governing a particular situation. In a vendor perspective the use of a checklist may be regarded as a business opportunity in terms of a legally founded security branding of offered solutions. Enhancing legal awareness among politicians and public officials for the purpose of efficiency, foreseeability, uniformity, openness, and so forth have other obvious advantages.

2 XML as a tool

The expression "XML as a tool" connotes markup languages in a broad sense, in particular SGML, considering the impact of this ISO standard dating back to 1986 on applications still running today. Furthermore, a markup language may be utilised for structural markup, styling, communication, and so forth. This implies that not only the core XML W3C Recommendation is of interest in this context but also related standardisations initiatives such as XSL, SOAP, and so forth. To conclude, XML ought to be regarded as a symbol for a system development approach that commonly includes data management in terms of text.

At one stage of the relatively short historical development of this type of applied information technology, the SGML community was a fairly closed community, not particularly open-minded to discussions about, for instance, pros and cons of various database technologies. Today, the situation has changed dramatically. XML can be said to play a central role in any technical solution involving web technologies, telecommunications, conventional electronic data processing, and to some extent
techniques having their origin in artificial intelligence. The term “docware” may, in this context, be used as a label for XML-related technologies that clarify the chosen approach of document management in a given situation.

All of this may, no doubt, be trivial to the previously experienced user of the above-mentioned family of standards. However, practical experiences show that a common misunderstanding at the management level of an organisation, be it a private enterprise or a public agency, is that XML (understood widely) involves a choice of a particular system design and possibly even software product.

Representatives of the industry, as well as other promoters of standardised markup languages, thus have a pedagogical task in explaining the underlying ideas of a non-proprietary approach to data management. Otherwise, there is an obvious risk that such a lack of understanding may be a major obstacle in widespread use of XML. In fact, there may be possible legal advantages associated with awareness of the inherent capacities of XML. The choice of system development approach, as such, may have an impact on a court's assessment of, for instance, whether an organisation's archival system is to be regarded as accurate or negligent in terms of meeting legal requirements of evidence by means of keeping track of version dependent legacy data. The pharmaceutical and automobile industries are typical examples of organizations heavily burdened by legal requirements of documentation. However, it may not be a trivial task in litigation to explain to a court just how the use of XML manifests a party's legal awareness.

To summarise, although XML may be described as a tool, it is not a physical object like a pen or a piece of paper. Neither may XML be described as a mechanical mechanism in the form of, for instance, the functions of a typewriter. Instead, XML is a tool with strong infrastructural potentials that are closely interlinked with IT-support for information retrieval, document management and knowledge management. From a legal position, this deserves particular attention.

Infrastructural changes

The term infrastructure is often used to describe the fundamental functions of society. It can refer to both 'hard infrastructures,' such as the road system, or 'soft infrastructure,' such as, social systems and various types of information systems. The basic components of a legal infrastructure, which may be regarded as 'soft’ according to the above-mentioned classification, include various forms of (a) data processing, (b) documentation, (c) communication, and (d) organisational forms.

The introduction of information technology into society has brought about dramatic changes to all these components. For example, data processing, a manual activity in the past, was transformed step-by-step during the 1970s and 1980s into automated data processing of cases. Today, automation of administrative activities involving legal decision-making based wholly or partly on automated routines, is a characteristic feature of administrative procedures. Another type of legal data processing takes place in connection with the development and conclusion of contracts. The technical possibilities of an electronic

---

2 In the documentation for ‘En hearing om den ‘mjuka’ IT-infrastrukturen (informationsinfra-strukturen) anordnad av IT-kommissionen’ this distinction between hard/physical infrastructure and soft/information infrastructure is described in the following way: “Sweden is building today advanced physical IT-infrastructure which will cover the whole country in the future. In addition to this physical infrastructure, ‘soft infrastructure’ is necessary in order to ensure dynamic exchange of services, which is so important for future economic growth. Soft infrastructure refers to both information and the fundamental services, such as, addressability, identification and security. How shall quality and functionality be guaranteed for embracing infrastructure?”, SOU 2000:123, p. 5.
conclusion of contracts, with the whole world as a marketplace, warrants a discussion in this area concerning the fundamental legal principles underlying offers, acceptance, evaluation of evidence, and so forth. Obviously, XML has a role to play, considering its potential for handling version-dependent text units over time, as a tool for improved legal system management. Earlier generations of lawyers would have naturally associated the concept of 'documentation' with physically demarcated paper documents, geographically located. In the age of the Internet, it is no longer obvious that documentation consists of paper documents, but that it may come in different forms of electronic documents, and in many cases carriers of declaratory acts, proprietary rights, criminal acts, and so forth. XML clearly mirrors this development. Mention should be made here of such initiatives as XML Signature that explicitly addresses the need for incremental signatures, which, for instance, may be of relevance in successive drafting of contracts.

In a similar way, (voice based) analogical communication services are less frequently used in legal work. Both civil servants' communication with their citizens, and lawyers' contacts with their clients are increasingly dependent instead on digital and mobile services. For instance, in Sweden, the comprehensive systems for the dissemination and collection of information by the authorities are based on a strategy that may be referred to as a kind of XML-labelling. The system for Dissemination and Collection (Sw. SHS) constitutes the public administration's investment in creating a general communication link to secure information exchange through the open Internet. In contrast to electronic trading systems, which are usually designed with a focus on business transactions in a certain sector, SHS constitutes a general platform that is not especially programmed for a certain sphere of activity.

As regards organisational forms, we have a strong tradition of working with nationally well-demarcated larger and smaller entities. This is especially clear in the information system of public administration which has developed harmoniously with nationally-defined government authorities, which are divided into central and local organs, and so forth. Information technology, as such, and the Internet, as a concept, have provided leverage for loosening up boundaries between authorities as well as national demarcation lines. In recent years, the private sector may be characterised by even more all-embracing, network-based and global organisational forms. It is evident that XML applied supports or rather is an integrated part of this infrastructural shift. Obviously, this give rise to a whole series of substantive law issues. For instance, how to apply privacy legislations on transborder flows of personal data.

3 Legal validity

3.1 Electronic signatures

There is no doubt that electronic signatures and other means for secure electronic messaging are becoming established in society. This development gives rise to a number of different legal questions. The main issue being the question of whether an electronic signature can bring about legal effects at all.

The implementation of the EC Directive on a Community framework for electronic signatures (1999/93/EC), that was adopted on 30 November 1999, and effective from 19 January 2000, and had to be enforced by the Member States by 19 July 2001, at the latest, clarifies certain legal situations. However, the manifestation of the development of law represented by this normative document is probably of even greater importance. There is still a lot of work to be done before computer transactions can be performed,

with the help of modern information and communications technology in a sufficiently secure way, on a daily basis. The latter expression refers to the necessity of minimising uncertainties as regards both different legal issues and practical (partly technical) circumstances surrounding electronic handling of documents. Business models and administrative traditions have not yet been fully adapted to the modern, more secure methods of information exchange.

The EC Signature Directive contains provisions relating to the legal effects of electronic signatures and the organs that may be able to offer electronic certificates that verify the genuineness of such signatures. This legislative novelty derives from article 5 of the Directive:

Legal effect of electronic signatures:

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:
   
   (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
   
   (b) are admissible as evidence in legal proceedings.

2. Member States shall ensure that an electronic signature is not denied legal effectiveness or admissibility as evidence in legal proceedings solely on the grounds that it is:

   - in electronic form, or
   - not based upon a qualified certificate, or
   - not based upon a qualified certificate issued by an accredited certificate-service-provider, or
   - not created by a secure signature-creation device.

The overall objective of this Directive may be said to co-ordinate the legal and technical work of the Member States as regards electronic signatures, removing in this way the obstacles to the internal market, especially in regard to electronic trade.

The main question of law is whether, how, and to what extent electronic signatures can be given the same legal effect as handwritten signatures. This will ultimately lead to the question of the evidentiary value of electronic signatures. This paper does not aim to provide a detailed analysis of these questions in the light of different jurisdictions. Here it will be sufficient to say that, in general, civil law has a relatively limited number of formal requirements concerning handwritten signatures. Typical examples, where such signatures are required, include consumer credits and real-estate purchases. In family law, testamentary dispositions and marital property agreements are often not valid without handwritten signatures. In administrative law, it is more common to require a a signature since processing of cases often presupposes submission of signed documents.

---

4 The following are examples of references in which this type of questions are treated in more depth: SOU 1996:40 (Elektronisk dokumenthantering), Ds 1998:14 (Digitala signaturer – en teknisk och juridisk översikt), Elektronisk dokumenthantering; en rättlig problemorientering, published by the Riksarkivet and Lagerlöf & Leman. Cf. also Bill 1999:2000:117, p. 14-18. In this context also Hultmarks Elektronisk handel och avtalsrätt (1998) should be mentioned, in which the author discusses, among other things, the ways in which different formal requirements in national law relate to UNCITRAL’s model enactments on electronic trading.
Nordic law

In this respect, applicable Nordic law shows that when the legislator uses the concept of 'written', electronic communication may be allowed to take place. The requirement of written procedure is posited here primarily as opposed to oral procedure. At the present stage of technical development, when a statute contains expressions such as 'signature,' or 'that must be signed by the party in question,' or the like, then it cannot be interpreted that electronic documents or signatures may be allowed to replace traditional paper documents and manual signatures. Special rules or established practice, however, may permit the use of electronic form after all.

As regards evidentiary value, the state of law is a bit clearer. There is no doubt that the principle of free examination of evidence characterises Nordic law. In general terms, this means that there are no limitations on the sources of evidence that may be used at a trial, and that a judge is not bound by any special regulations regarding the way different types of evidence shall be evaluated. Neither does the legislator seem to wish to introduce any general rules on the burden of proof that would be dependent on the medium used in a given case. Instead, the important factors are considered to be the parties' internal relations, the character of the legal document, and so forth.5 One can therefore conclude that Nordic courts encounter no formal obstacles to considering system evidence in the sense of electronic documents, electronic signatures and other components of information systems.

To return to the EC Directive, it does not address the question of entering into contracts in electronic form. Neither does the Directive examine any of the so-called closed systems in which the use of electronic signatures is based on voluntary agreements under civil law between specific parties, concerning the conditions for the handling of data (see, point 16 in the Preamble).

Notwithstanding the above, the Directive is innovative from the European perspective by virtue of the fact that electronic signatures have been granted legal enforceability, which was not the case earlier in those countries that lack the principle of free examination and evaluation of evidence. Instead, the primary innovation, with regard to Sweden, is the authority that accompanies, under certain circumstances, application of the rules focusing on the parties providing electronic certificates.

3.2 XML related security-enhancing factors

The discussion above boils down to the need for a strategy to handle the legal uncertainty characterising the electronic society and illustrated by the EC Signature Directive. This manifested need for a legal strategy may, in practical terms, be transformed to a focus on XML related security enhancing factors. The table below presents an overview - not an exhaustive list - of what here is referred to as XML characteristics, means and legal incentives.

5 Bill 1999/2000:117, p. 18
### 1. XML characteristics

<table>
<thead>
<tr>
<th></th>
<th>2. Means</th>
<th>3. Legal incentives</th>
</tr>
</thead>
</table>
| Non-proprietary format | Inherent in any XML application                                         | **Public sector:** Accessibility in a long-term perspective  
Private sector: Legal requirements of keeping track of legacy data |
| Quality assurer in document production | Validated documents by means of DTD:s and schemas | **Public sector:** Public information supply (possible state responsibility)  
Private sector: Commercial products (avoiding liability) |
| Quality assurer in document distribution | One single repository as a basis for customizing production on, e.g. CD-ROM, on-line, print | Public sector: See above  
Private sector: See above |
| Container of legal directives | Markup vocabularies                                                      | **Public and private sectors:**  
- Availability differentiator (Official or secret data)  
- Authority indicator (Mirroring acting parties authorities)  
- Property rights administration⁶ (Labelling of rights and its owners) |
| Secure electronic messaging | For instance, XML Signatures or mathematical approaches to incremental signatures of structures and marked up documents | **Public and private sectors:** Normative as well as other legal requirements of authentication, validation and signed documents (text entities) |

### 4 Security context

In the area of information security, a number of different criterias are usually laid down as the starting point for risk analyses and decisions as to whether an adequate level of security has been reached. Frequently recurring criteria include: (a) availability, (b) confidentiality (secrecy), (c) data integrity (d) accountability, and (e) non-repudiation.⁷ The objective of electronic signatures is to cover this type of security aspects. In practice, the main purpose is to identify the sender of the electronically transmitted information, who shall not be able to deny the fact that it was he or she who initiated the transmission, and, not less importantly, to establish whether the transmitted information has been distorted in any way.


An important demarcation line concerning the different circumstances characterising the use of electronic signatures pertains to the question of whether the so-called closed system is concerned that the parties have agreed right from the start upon the forms of information transfer, or whether the so-called open system is concerned that the parties are unacquainted with each other to start with. Companies' internal systems, as well as certain sector-specific systems, in which the use of, for example, EDI, has been regulated by agreement, constitute typical closed systems. Obviously, Internet transactions, in which persons exchanging information cannot be expected to know each other in advance, are to be regarded as events in an open system. Nevertheless, Internet usage does not automatically entail anonymity of the parties involved. More frequently, there is some form of agreement between customer/supplier, customer/store, etc., as a basis for the electronic transactions performed.

In the era of IT-supported document management there is a growing need for version control in a long-term perspective. Document markup, including linking techniques of different kinds, is attractive as a general value-adding method. At the same time, the introduction and widespread use of increasingly advanced digital document management systems is resulting in a very complex environment for text handling. Furthermore, open systems are a major development trend in today's communications networks. Therefore, one important concern, is how best to secure trails of authorisations, alterations included. More precisely, this is a matter of information security policies mirroring the norms that govern an organisation, such as, who has a right of access to what, without knowing beforehand who will be claiming this right of availability.

Considering that the major characteristics of normative documents are complex, interdependent text units, shifting in content over time, interpretable only in context, we can extract one key issue, and that is the question of a methodological approach to regulatory management. If the challenge in terms of a required infrastructure is overcome, we can indeed expect the added value so often promised by vendors. There is otherwise an obvious risk of turning back or, perhaps, even failure.

The cornerstones in a system development approach that meets the fundamental requirements of modern regulatory management as a vital aspect of information security are: (a) document markup, (b) information security, and (c) legal awareness. XML naturally represents the core method regarding document markup. From the point of view of regulatory management, XML offers vital possibilities of transparent modularity in a structural context. The conventional understanding of information security is that it comprises confidentiality, availability, integrity, accountability, and non-repudiation. Ongoing work at IETF on securing web-based documents will, of course, serve as an important input. In this context, focus is on the XML Signature and Encryption initiatives. The application of a cryptographic method of progressive (incremental) security enhancement may serve as supplement. Finally, legal awareness is required both in terms of methodological aspects of legal system development and of substantive law issues related to the use of digital signatures, evidence, and so forth. The last mentioned perspective might also be expressed in terms of possible legal validity as proof of actions of different kinds.

The approach described above serves as a basis for the so called SLIM Project - Secure Legal Information Management - hosted by the Faculty of Law at Stockholm University that will occur during the period 2002-2005 (see http://www.juridicum.su.se/slim). The SLIM project is founded mainly on previous practical and theoretical experiences using SGML in the legal domain - the Corpus
Legis project (see http://www.juridicum.su.se/iri/corpus) together with expertise from the Department of Information Theory at the University of Lund and Swedish Institute of Computer Science (SICS).

Because of the early stage in commercial tools that combine XML capability and digital security enhancing techniques, one aim of the SLIM Project is to have an impact on the development of future commercial XML tools for legal purposes.

**Concluding remarks**

The discourse of this paper is based on the standpoint that XML may be regarded as a **tool for legal validity in a security context**. The point is made that XML ought to be broadly understood and that the tool metaphor has implications beyond trivial physical and mechanical ones. In terms of general development trends we have reflected upon how XML has become an integral part of modern infrastructures, with obvious legal implications. More precisely, this has a bearing on modern means for data processing, documentation, communications, and organizational forms.

The practical situation of today is illustrated by a brief discussion on the EC regulative approach to electronic signatures. The fact that there are still so many legal uncertainties, in terms of lack of foreseeability, concerning legal validity of actions of various kinds calls for special attention. A pragmatic approach is presented regarding various XML characteristics as security enhancing factors.

To conclude, the attraction of combining XML with conventional security-enhancing methods lies in the need for transparent, content dependent and context sensitive management of legally relevant text units over time. In this context, legal awareness may indeed enhance information security.
References


Ds 1999:73 Elektroniska signaturer.

Digitala signaturer på väg: Krypterade smartkort ska skydda e-shoppare, deklaranter och företag. In Ny Teknik no. 5, 2001, p. 16-17.


Prop. 1985/86:80. Om ny förvaltningslag (Bill: New administration act)

Prop. 1999/2000:86. Ett informationssamhälle för alla (Bill: One information society for all)

Prop. 1999/2000:117. Lag om kvalificerade elektroniska signaturer, m.m. (Bill: Act on Qualified Electronic Signatures Act, etc.).

Skår, Nicklas. Lag om elektroniska signaturer: en lag som inte behövs? In: Industriforum 4, 2000, p. 21

SOU 1990:37. författingsreglering av nya importrutiner m.m. Delbetänkande av utredningen om lagstiftningsbehovet av tulldatoriseringen (TDL-utredningen).


