Managing Electronic Signatures – Current Challenges

Cecilia Magnusson Sjöberg &
Anna Nordén

Borttaget:

Borttaget: Working

1 Introduction

1.1 Chosen approach

In a legal environment electronic signatures are commonly presented as a means for meeting formal requirements of document management. This implies a need to consider substantive law governing various activities in society.[1] Rules and regulations on how to sign a document are found within a wide variety of legal fields including family law, real estates, taxation, consumer rights, etc.

Borttaget: and practical

There is a continuously developing *legal framework* directed towards acceptance of use of electronic signatures for legal purposes. The EC Signature Directive 1999/93/EC[2] (the “E-Signature Directive” below) is of course an important contribution, but it has unfortunately not led to the clear and harmonized situation hoped for.

Borttaget: equal to handwritten ones

Electronic signatures are intrinsically different from handwritten ones in that they may be taken advantage of for many different kinds of security enhancing measures. Associated technologies offer, namely, ways to ensure data integrity, non-repudiation, confidentiality etc, which are relevant features both in a pure technical security enhancing perspective, as well as when a handwritten signature needs to be replaced in electronic networks of different kinds.

In order to minimize the risk for legal uncertainties there is a need for awareness of how electronic signatures function; how to use them in a similar way to handwritten ones, and what to be cautious of. Although the paper metaphor might by tempting to use as an explanatory model, it may in fact cause more harm by confusing concepts rather than contribute to a deeper understanding of what can and cannot be accomplished by electronic signatures. It is also vital to remember that not all use of electronic signatures have the same aim as handwritten signatures in the paper world, in which cases the paper metaphor can be directly mis-leading.

Borttaget: therefore

Borttaget: e

Borttaget: s

Borttaget: metaphore

Borttaget: but

Borttaget: concpets

Borttaget: deaper

Borttaget: y

A starting point for this article is that *managing electronic signatures* is a critical factor in the context of e-commerce including electronic communications, both in B2B and with public agencies. This analysis of electronic signatures will therefore place an emphasis on *practical issues from a legal point of view*, whether electronic signatures are used for legal purposes (e.g. signing of contracts) or merely as a security method (e.g. integrity check of data signed).[3] The title “Managing electronic signatures” highlights the importance of a legal approach not only addressing rules and regulations but also challenges in the context of *implementation*.

Borttaget: artickle

Formaterat

Borttaget: as well as in

Borttaget: r

Borttaget: indicates

Regardless of electronic signatures being a feature of the modern information society there is every reason to revisit the notion of *legal system management*[4].

[1] *See e.g.* the Swedish government report Ds 2003:29, *Formel: Formkrav och elektronisk kommunikation*.

[2] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[3] *Cf.* Mason, Stephen, *Electronic Signatures in Law*, LexisNexis Butterworths, 2003 “http://www.lexisnexis.co.uk/”.

[4] *See* Seipel, Peter, *Computing Law*, Stockholm 1977.

Historically, legal system management addresses core components in legally well-founded automatic decision-making,[5] information retrieval,[6] and electronic document management[7]. The use of information technology (IT) for the above mentioned purposes can be related to the legal domain either directly, e.g. an application for knowledge management in a business law firm, or indirectly, e.g. an electronic market place where actions taken have legal implications. More precisely, legal system management takes into consideration system design as well as system management. Let us now reflect upon electronic signatures in the same way, but first a few terminological remarks.[8]

1.2 Terminology etc.

Although there are differences, an electronic signature is often equalled with a digital signature.[9] For this reason this article to will use the word electronic signature as a synonym for digital signatures unless otherwise explicitly stated.

Borttaget: d

Depending on practical circumstances it might be, however, important to elicit major forms of signatures. To begin with a major distinction is to be made between digital signatures and imprinted signatures (conventional ones). An *imprinted signature* may in a historical perspective be regarded as the conventional form of signing. It can be implemented manually (e.g. using pen and paper), mechanically (e.g. with the aid of a robotic) or, by biometric means (e.g. a finger print).

A *digital signature* is based on algorithms and mathematical procedures. It can be implemented in many ways, for instance, by way of using an electronic computer (e.g. a PC), a mechanical computer (e.g. a calculating machine), an optical computer (e.g. based on light) or, manually. One understanding of an *electronic signature* is that of a digital signature implemented by means of an electronic computer.

Within the *legal domain* the notion of electronic signature has evolved into a concept denoting digital signatures implemented in electronic computers with certain legal implications. It may be questioned whether this phrasing of normative instruments is wise considering the risk for placing too much emphasis on technical aspects instead of methodological ones.

[5] *See e.g.* Magnusson Sjöberg, Cecilia, *Rättsautomation: Särskilt om statsförvaltningens datorisering*, Stockholm 1992 and Schartum, Dag Wiese, *Rettssikkerhet og systemutvikling i offentlig forvaltning*, Oslo1993.

[6] Including advanced legal information retrieval based on probabalistic methods.

[7] *See e.g.* Magnusson Sjöberg, Cecilia, *Critical Factors in Legal Document Management*, Stockholm 1998.

[8] This article is partly based on ideas presented in the conference proceedings *EU Electronic Commerce Law*. Eds. Ruth Nielsen, Søren Sandfeld Jacobsen and Jan Trzaskowski, p. 95-98, Copenhagen 2004. For other aspects *see e.g.* Kronqvist, Stefan, *Brott och digitala bevis: En handledning*, Stockholm 2003, Udsen, Henrik, *Den digitale signatur – ansvarsspørgsmål*, Köpenhamn 2002.

[9] *See e.g.* the Swedish e-banking solutions such as BID, Nordea etc.

Borttaget: ,

Public Key Cryptography

A *Public Key cryptography System (PKS)* is based on a method combining pairs of so-called public keys and private keys. A PKS uses *asymmetric encryption*. The model is based on the assumption of a *public key* being made generally available while the *private key* only is to be used by the holder of it. This allows for signing processes in networks in which you do not know signing parties in advance. It should not be disregarded, however, that a PKS might be used by way of transferring a public key (as a credential) to someone particular. This approach encompasses a certain amount of *non-mechanical trust* in the actual reliance of the holder of the public key.

The PKS-model is, furthermore, based on the assumption that the private key is kept secret. Problems of evidence may, of course, occur as a result of a secret key not being kept secret in a proper way, which may open up for uncertainties as regards non-repudiation, etc.

A PKS supports authentication, data integrity and non-repudiation in the form of only one person having the possibility of signing with the private key.

Public Key Infrastructure

In practice a *Public Key System (PKS)* takes advantage of a *Public Key Infrastructure (PKI)* to make it trustworthier. The overall purpose of a PKI can be described as guaranteeing the identity related to a public key. In practice this is accomplished by a so-called *trusted third party (TTP)*[10] – could be a *certification authority (CA)* within the public or private sector – signing public keys, and thus vouching for the link between the private key and a physical or legal person.

Borttaget: *otherwise it is difficult*

A certain amount of *non-mechanical trust* lies in the role of the TTP.

Symmetric Key Cryptography

Symmetric Key cryptography System (*SKS*) uses a secret key being exchanged among the users. This implies that the secret key cannot be totally confidential. Everyone having access to it may use the secret key in the same way. Symmetric encryption thus supports data integrity but not non-repudiation.

In comparison with a PKS, an SKS is generally more suited for data encryption. In practice the two methods are almost always used in combination; the PKS is used for authentication; signing and key exchange while the SKS is used for encryption of the session or document.

[10] Note that a public key system does not necessarily presume the involvement of a third party.

2 Major Legal Framework

The E-Signature Directive elaborates on legal effects related to different security levels of electronic signatures. These effects range from a non-discrimination rule applicable to any electronic signature, to mandatory handwritten signature-equivalence for so called qualified electronic signatures[11]. An electronic signature according to the E-Signature Directive is data associated with other data and “which serve as a method of authentication”[12], without specifying any technical means of how this should be achieved. In addition to the wide and technology-neutral definition of an “electronic signature”, the E-Signature Directive includes a definition of an “advanced electronic signature”.[13] The definition does not explicitly include a requirement for the signature to be based on PKI, although PKI is implicitly the technology the EU legislator had in mind when defining the advanced electronic signature.[14]

Borttaget: ,

Borttaget: certificates etc

Borttaget: c

Borttaget: (Public Key Infrastructure) technology

Current reports show, however, that comparatively few qualified certificates have been issued.[15] This fact, in combination with a common misunderstanding of the E-Signature Directive – a qualified electronic signature is *not* a synonym for “legally valid electronic signature” but is only one way, to get the rules on handwritten signatures to apply – has led the E-Signature Study for the European Commission to recommend to discourage EU member states from inserting references to qualified electronic signatures in national legislation.[16] This strange paradox, i.e. that qualified electronic signatures are discouraged and not used by a large majority of EU persons, while some countries at the same time insist on requiring such signatures, is of course unfortunate for the development of e-signature use and the Single Market.

Borttaget: so called

Borttaget: signatures

Borttaget: to the advice

Borttaget: that

Borttaget: to

Borttaget: by the EC

A common mix up in discussing electronic signatures is the use of electronic signatures as an information security technology, with the aim to ensure integrity and authenticity of the signed data, and the use of signatures as a legal concept trying to replicate the handwritten signature in the paper world. These two different “uses” or aspects of electronic signatures have created a lot of confusion – many think of an electronic signature only as a legal concept meant to replace the handwritten signature, and forget that signatures are as often used primarily to e.g. ensure the integrity of documents in electronic transfer.[17] One

[11] A “qualified electronic signature” is not a concept in the Directive but a definition used by lawyers and national legislators to define an advanced electronic signature based on a qualified certificate and created using a secure signature creation device, *see* Article 5.1 in the E-Signature Directive and *The Legal and Market Aspects of Electronic Signatures*, Jos Dumortier et.al. Study for the European Commission – DG Information Society, Leuven 2003.

[12] Article 2.1 Directive 1999/93/EC.

[13] Article 2.2 Directive 1999/93/EC.

[14] In earlier draft versions of the E-Signature Directive the term “digital signature” was used. *See* also *The Legal and Market Aspects of Electronic Signatures*, Leuven 2003 p. 30.

[15] *See* further *The Legal and Market Aspects of Electronic Signatures*, Leuven 2003.

[16] *The Legal and Market Aspects of Electronic Signatures*, Leuven 2003 p. 12.

[17] This problem arose when paper turned to electronic documents and people got confused and took the paper world concept as the leading notion, instead of thinking only in functional terms.

area in which this problem is particularly flagrant is in relation to electronic invoicing and the VAT Directive 2001/115/EC (the "VAT Directive").[18]

As mentioned above, the E-Signature Directive is a cornerstone of the legal framework for accepting and promoting use of electronic signatures. Interestingly, second level legislation that refers to this Directive is now emerging. Examples are the VAT Directive that regulates electronic invoicing, and the E-Procurement Directives 2004/17/EC[19] and 2004/18/EC[20] that include security requirements for electronic public procurement. This emerging legislation does however create certain ambiguities, a lot due to the uncertainties of the E-Signature Directive. Of particular interest in this context is that Directive 2004/18/EC includes a reference to the E-Signature Directive by way of allowing member states to require that electronic tenders be accompanied by a qualified electronic signature (an advanced electronic signature based on a qualified certificate and created using a secure signature creation devise).[21]

Borttaget: of

Borttaget: s

Borttaget: n

A key issue in the VAT Directive is whether or not an electronic invoice must be electronically signed by a specific individual or if it is sufficient that a legal person "signs" or "stamps" the invoice. The VAT Directive uses the advanced electronic signature concept of the E-Signature Directive as a means of achieving authenticity and integrity. The aim is not to apply a handwritten-equivalent to the invoice, but rather a "security-stamp" for the purpose of guaranteeing that the origin of the invoice can be established and that the invoice has not been changed or tampered with.[22] This is not surprising but rather expected – a paper invoice is normally not signed with a handwritten signature but printed on a paper with an organization letter head, and the VAT Directive is looking for the same functionality in the electronic world. However, due to certain national implementations of the E-Signature Directive that restrict the use of advanced electronic signatures to natural persons, a legal person will in many cases be prohibited to secure the invoice with an organizational electronic signature.[23] This is particularly unfortunate in many industries where automation of electronic invoices is important. The legislative confusion around electronic

Borttaget: Furthermore, *legal uncertainties* remain in spite of this EU initiative e.g. within the taxation area.

Borttaget: s

Borttaget: electronically signed

Borttaget: -

Borttaget: associated with

Borttaget: merely

[18] Council Directive 2001/115/EC amending Directive 77/388/EEC with a view to simplifying, modernizing and harmonizing the conditions laid down for invoicing in respect of value added tax, Official Journal L 015, 17/01/2002 P. 0024-0028.

[19] Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors.

[20] Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts.

[21] Article 42 p 5 b of Directive 2004/18/EC has the following reading: Member States may, in compliance with Article 5 of Directive 1999/93/EC, require that electronic tenders be accompanied by an advanced electronic signature in conformity with paragraph 1 thereof.

[22] The VAT Directive expressly prohibits member states from requiring that electronic invoices be "signed", Article 2.2 Directive 2001/115/EC.

[23] *See* further ICC comment on the use of advanced electronic signatures by legal persons for security purposes, March 2003, Commission on E-Business, IT and Telecoms Task Force on Security and Authentication, Doc 373-36/4, Paris 2003.

invoicing is one example of issues that need to be taken into account in the implementation of electronic signatures.

3 Implementing Electronic Signatures

Evidently, the choice of system development approach for an implementation of electronic signatures is *application area dependent*. Implementing electronic signatures for the purpose of e-invoicing is quite different from contract management or product data management, although the signature in all these cases is aiming for technical security. Yet different is implementing an e-signature for a legal act such as signing a contract. In addition to various *application areas* a system development approach is dependent on *sectoral* aspects. For example, the application of data protection legislation varies between the public and the private sectors of society. Furthermore, an implementation of electronic signatures in the public sector must take into consideration principles of openness and rules governing administrative procedures. Broadening the perspective even more, *jurisdictional* aspects need to be considered; will an implementation of electronic signatures be utilised only within the EU and/or in so called third countries? *Technical and organisational* matters have an impact also on the choice of system development approach; will transactions secured and/or signed by electronic signatures take place in open and/or closed networks?

A major task related to all the above-mentioned aspects of system development approach is, of course, to ensure *legal validity* of electronic signatures – again, whether they are used for legal acts or for mere (information) security purposes.

Borttaget: , etc

Borttaget: *topic*

Borttaget: into consideration

Borttaget: based on

Borttaget:

Borttaget: ,

4 System Design

4.1 Conceptual Model of Legally Relevant Building Blocks

After having captured an appropriate *system development approach* the next phase of an implementation of electronic signatures is *system design*. A *conceptual model of legally relevant building blocks* will support this process. Without going into any detailed (technical) explanations, the list below comprises *core concepts (C) and actions (A)* related to electronic signatures:

Electronic identity (C)

States that a certain user (physical or legal person) is the holder of a specific public key, for instance, by using a certificate provided by a trusted third party (TTP)

Electronic identification/authentication (A)

Confirmation of electronic identity at a specific time, for instance, by using passwords or an electronic signature

Formaterade: Punkter och numrering

Formaterade: Punkter och numrering

Formaterade: Punkter och numrering

Formaterade: Punkter och numrering

Borttaget: digital

- Signature object (C)
  - For example, an e-invoice, a contract or product data
- Electronic signing (A)
  - Process comprising the calculation of data extract to be encrypted by a private key
- Electronic signature (C)
  - Encrypted data extract attached to the signature object
- Electronic verification (A)
  - Process comprising the calculation of data extract of signature object and decryption of signature data, and also comparison of hash sums
- Electronic encryption of signature object (A)
  - Ensuring confidentiality
- Electronic decryption of signature object (A)
  - Ensuring confidentiality

Formaterade: Punkter och numrering

Formaterade: Punkter och numrering

Formaterade: Punkter och numrering

From the listing above it becomes clear that one should not be fooled by a *handwritten”digital” signature,* i.e. an image of a pencil drawn signature that has been transformed into a computer readable format, for example, by scanning. Such a signature is not dynamically related to the signature object in the way a digital signature is. This somewhat trivial comment points at the importance of grasping the *functionality* of electronic signatures (in a broad sense).

Borttaget:

Electronics signatures may be implemented in many ways depending on the application area. As mentioned above a so-called *Public Key Infrastructure (PKI)* is a model that has heavily inspired the European Union normative initiative. From a general business point of view (including legal considerations) it is of vital importance to analyse which information security functions a chosen model supports. For instance, an implementation of electronic signatures based on a PKI supports authenticity, control of data integrity and non-repudiation (in a technical sense). It does not, however, support data integrity (protection against distortion of data) and confidentiality (protection against unauthorised access to data), although a PKI implementation for e-signatures also gives encryption possibilities.

Borttaget: so called

Borttaget: governed not the least

Borttaget: of

Borttaget: .

In practice, not only the legal implications of the overall implementation model but each entry in the list of core concepts and actions (above) need to be considered. To exemplify, many e-business activities include a wide variety of *signature objects*. It is no doubt a worthwhile task to structure key signature objects according to their major characteristic from the point of view of signing. The list below illustrates a variety of possible signature objects.

Borttaget:

- Record/Document
  - Fraction
  - Singular
  - Collection
- Case
  - Process oriented data

Formaterade: Punkter och numrering

- Messages
  - E-mail
  - Attachments
- Transaction
  - Business oriented data
- Context
  - For example, authentication data
- Version
  - Content
  - Format
- Links
  - Internal
  - External

Formaterade: Punkter och numrering

4.2 Extraction of Application-related Legally Relevant Information

Borttaget:

A conceptual model of legal building blocks may not only be taken advantage of for the purpose of a general analysis of core concepts and actions but also for extraction of *application-related legally relevant information*. In the context of e-contracting, it is, for instance, important to uphold a distinction between an electronically signed invitation to treat on the one hand and an electronically signed binding offer on the other.[24] In the context of e-invoicing it is important to distinguish between the electronic signature (or security "stamp") that a legal person may apply to ensure the integrity of an invoice, and a "signature" that is meant to replicate the paper world – EU member states are forbidden to require that an invoice be "signed" in the handwritten sense.[25] Furthermore, legal requirements including evidential aspects may call for various security levels of how electronic signatures are implemented. Here reference should be made to the E-Signature Directive (1999/93/EC) that includes provisions defining (simple) electronic signatures, advanced and what is referred to as qualified ones.[26]

Borttaget:

Borttaget: ¶

4.3 Digital Representation of Legally Relevant Information

In order to obtain a functioning implementation of electronic signatures in a technical environment the application-relevant information must be *digitally represented*. For this purpose there are, as mentioned above, several techniques

Borttaget: make an

Borttaget:

[24] *See* further e.g. Edwards, Lilian and Waelde, Charlotte, *Law & Internet: a framework for electronic commerce*, Oxford 2000, Fejø, Jens, Nielsen, Ruth, and Riis, Thomas, *Legal Aspects of Electronic Commerce*, Copenhagen 2001, and Ramberg, Christina, *Contracting on the Internet: Trends and Challenges*, Stockholm 2002 p. 109-116.

[25] Article 2.2 Directive 2001/115/EC.

[26] Note that the E-Signature Directive does not regulate the use and consequences of a qualified electronic signature, but only makes sure that it is, legally speaking, treated in the same way as a handwritten signature. See further *The Legal and Market Aspects of Electronic Signatures*, DG Information Society, Leuven 2003 p. 6.

available, which can be used alone or in combination. PKI-technologies, EDI-solutions,[27] data base technologies, information standards and web services[28] are just a few examples of components in today's technical infrastructures.

Borttaget: ¶

4.4 *Legal User Interfaces*

One dimension of implemented electronic signatures that should not be underestimated concerns what may be labelled as *legal user interfaces*. In fact, this notion manifests the need for legal system management that was established already during the 70ies (see introduction above), which during the following two decades evolved into theories of legal system development and legal standards. Today, it is even possible to find legal user interfaces as an explicit goal of public agencies.[29] Basically, it has to do with an awareness of the advantages of integrating legal aspects not only into preparatory system design work, e.g. focusing on governing legal frameworks, but also to allow legal aspects to have an impact on the final technical work, including user dialogues. By doing so prospects of well-founded trust in information technology will increase.

An approach to legal user interfaces oriented towards electronic signatures could, for example, aim at, (a) an acceptable level of functionality, (b) a reasonable level of complexity, and (c) assurance of information security. A successful implementation from this point of view might be that "you see what you sign", that user dialogues are comprehensible even for non-experts and that information security requirements are met not only from a technical point of view but also from a legal perspective, to ensure enforceability in a court of law. These points may appear to be simple and easy to accomplish, but in practice, as evidenced by the majority of current business applications, they are not.

Borttaget:

Borttaget: that

Borttaget: is upheld

Borttaget: taking

Borttaget: into consideration

Borttaget: ¶

4.5 *Concluding Remarks on System Design*

In a business environment an application involving electronic signatures involves various constellations of trusted as well as non-trusted parties. These actors might be known as well as not known. Obviously, it is important to illuminate *different roles and authorities* as clearly as possible.

Borttaget: t

Furthermore, the notion of "electronic signatures" is not to be mistaken for a singular function as it implies a whole *process of actions* based on legal, technical as well as business-oriented building blocks.

Borttaget:

Although PKI-technology did not meet the expectations that were raised when it was first introduced it is too early to out rule this approach. It is fair to say that what has disappointed is the proprietary approach underlying most traditional PKI offerings, which have created high thresholds for application

Borttaget: ,

[27] Electronic Data Interchange.

[28] *See* further e.g. Newcomer, Eric, *Understanding Web Services*, Boston 2002.

[29] *See* further SAMSET (Samhällets elektroniska tjänster), i.e. a Swedish initiative within the area of e-supported public services, "www.rsv.se/samset/samset/html".

integration and thus for testing of legally solid usage approaches. Now that the PKI industry is placing more emphasis on integration, interoperability and legal value, it may be timely to revisit *PKI* techniques. This review should take account of new methods for *identity management (IdM)*. A challenge in this context is no doubt to keep control of the level of *complexity*. This applies in particular to how electronic signatures are implemented from a user's point of view.

Borttaget: Rather

Borttaget: it appears to be time

Borttaget: in combination with

5 System Management

5.1 An Electronic Signature Strategy

A successful implementation of electronic signatures presupposes not only a system development approach and system design activities. After an application is brought into operation, the phase of *system management* begins. This could be expressed also as a need for an *electronic signature strategy* (e-sig strategy for short).

Borttaget: up and running

To illustrate, one critical factor in such an e-sig strategy is to decide upon storage object(s). With this view in mind, it might be important to differentiate between *various kinds of signature objects*, such as an e-invoice, a contract, product data, etc. A key point in today's discussion is whether to store or not to store the electronic signature itself and/or signature data. Signature data are here to be understood as contextual information on conditions for applying a signature, e.g. time, roles and authorities of individuals involved. A closely related question concerns for what duration, if any, there is a need to save an electronic signature and/or signature data.

Borttaget: how long

Borttaget: time

Legal requirements as well as business conditions and available technical tools govern an e-sig strategy. There are, for instance, comprehensive rules and regulations demanding long-term archival of original data within the pharmaceutical industry, laws requiring storage of electronic invoices for ten years, etc. Another reason for archiving electronic signatures is its potential as digital evidence in a future legal dispute.

Borttaget:

Borttaget: 10

Borttaget: court trial

Yet another incentive for an e-sig strategy may be found in business imperatives related to cost reduction or return on investments (ROI) as well as prospects of future business transactions.

Borttaget: o

5.2 An E-sig Method

An e-sig strategy needs to be supplemented with an *e-sig method*. The purpose may be expressed in terms of long term management of electronically signed data objects. Such a method must be based on technical solutions in combination with organisational ones. More precisely, it will support archival functions by way of *attaching* or *detaching* signatures. As pointed out before, certain aspects of signature data may be relevant for archival purposes. Verification data can, for instance, function as support for security assurance (a kind of contextual meta data). An e-sig method could also provide measures for *resigning* signature objects. Not every application will, however, demand archival of electronic signatures (in a broad sense).

6 Challenges

6.1 Dynamic Management of Electronic Signatures

The discussion above about system development approach, system design and system management boils down to a need for *dynamic management of electronic signatures*. Evidently, this is not trivial to accomplish. Just to mention a few *complicating factors* one individual may be associated with several organisational roles and at the same time be holder of a variety of authorities. Furthermore, a group of individuals may be authorised to sign the same signature object (e.g. an e-invoice, a contract, an electronically filed job application). One singular record may comprise a whole set of signed data fractions. In practice, many e-business applications are characterised by workflows of signed signature objects, etc.

One way of dealing with the challenges of electronic signatures is to *build trusted legal infrastructures*. The notion of legal infrastructure may be explained as those parts of a legal system that form the basis and conditions for legal activities. Trust has become a common denominator for evaluation of IT-applications. A somewhat deepened analysis of the trust concept shows that from a legal point of view it is necessary to differentiate between well-founded trust, un-founded trust, well-founded mistrust and un-founded mistrust.[30]

Borttaget: motivated

Legally applied information standards are another step towards dynamic management of electronic signatures. In this context *proactive law* plays an important role. This is, however, not to be understood as legislative actions but rather to let law play an active role in IT-related activities. One example worth mentioning is the development of legally oriented vocabularies that take advantage of information standards.

Borttaget: ,

Borttaget: of

Borttaget:

Considering the rapid development of e-business applications based on information standards it is worthwhile to here (briefly) present XML – Extensible Markup Language.[31] The core document markup standard XML is a W3C[32] Recommendation[33] with a whole family of related standards and vocabularies. For the purpose of document markup there is UBL (Universal Business Language). ebXML (e-business XML) supports messaging and with

Borttaget: motivated

Borttaget:

[30] See Further Magnusson Sjöberg, Cecilia, *Tillit i informationssamhället: Kejsarens nya kläder eller förändrade förutsättningar för rättsutvecklingen?* In Nordisk årsbok i rättsinformatik (NÅR) 2002 p. 107-125.

[31] *See* also e.g. Lundblad, Nicklas and Magnusson Sjöberg, Cecilia, *Making Money from Information Standards.* In: XML Europe 2003, 5-8 May, 2003, London, Conference Proceedings. 22 ff. Electronically available at "www.lisan.org" (publications).

[32] World Wide Web Consortium.

[33] *See* further www.w3.org/TR/REC-xml.

the prospects of enhancing information security there are XML encryption, XML digital signatures and SAML (Security Assertion Markup Language).[34]

XML offers an expressiveness that enables contents markup etc. far beyond what is possible to accomplish with HTML (Hyper Text Markup Language). This is of vital importance considering that legal information is not just any kind of information.[35] The inherent possibility of validation of applied markup is a true advantage considering the special data quality demands related to the management of legal information.

An XML document can be well formed or governed by either a so-called DTD (Document Type Definition) or schema. The document instance comprises the encoded document containing subject-oriented data (e.g. legal text), markup (element tags and attributes) and a DTD reference. The text below illustrates a marked up text unit in the Data Protection Directive (95/46/EC) including element tags and an attribute (ID).

```
<ARTICLE ID='A3-95-46-EC'>
<ARTTITLE>Scope </ARTTITLE>
<ARTNO>Article 3 </ARTNO>
<PARA> 1. This Directive shall apply to the processing of personal data wholly
or partly by automatic means, and to the processing otherwise than by automatic
means of personal data which form part of a filing system or are intended to form
part of a filing system.> </PARA> ...
</ARTICLE>
```

As a tool for digital signatures XML offers a variety of *signature methods*.[36] In comparison with conventional monolithic methods that do not allow for diversity XML-based approaches are more selective. A major advantage is the possibility to use previously structured and marked up text units. Of course, one has to consider the implications of signature implementation – attached/detached (see figures 1 and 2 below) – in this technical environment too. What are the consequences, with regard to, *storage requirements* depending on archival time, whether or not data must be unchanged, needs for data migration and accessibility requirements; who will use the signature data and how will it be used, etc.? All this will have an impact on the technical implementation in terms of software, operating system, network solutions, etc.

Borttaget:

Once again there is reason to return to a legally oriented discussion about trust (see above). There is no doubt that XML offers a basis for *well-founded trust* in its validation methods that could be applied for control of whether a stipulated electronic signature has been inserted or not.

Formaterat

At the same time there is a risk for *un-founded trust* in the possibility of segmented signing of marked up text units out of context. It might, for instance, appear to be security enhancing to electronically sign a given consent to personal data processing. However, a legally valid consent must according to EC Data

Formaterat

[34] *See* further e.g. Ray, Erik T., *Learning XML*, Sebastopol 2003 and Chiu, Eric, *ebXML Simplified*, New York 2002.

[35] Introducing XML into the legal domain requires awareness of how different legal sources relate to each other according to their norm hierarchical status, etc.

[36] *See* further XML-Signature Syntax and Processing, "www.w3.org/TR/xmldsig-core".

Protection legislation be explicitly associated with additional information of what kind of personal data processing a data subject has consented to as well as the overall purpose of the processing.[37]

Furthermore, *well-founded mistrust* may be raised as regards the complexity associated with the variety of methods available to accomplish a so-called normalised form of signature data, which serves as the basis for "hashing"[38] the signature data previous to its encryption.

Formaterat

Finally, *un-founded mistrust* has quite often been directed to the use of information standards, not the least XML, as requiring certain system design solutions in spite of its technical platform independence. On the contrary, information standards represent a method – and not a given solution beforehand – for document management. Generally speaking, information standards can be taken advantage of for messaging, contents management as well as for security enhancement. The challenge lies in its implementation.

Formaterat

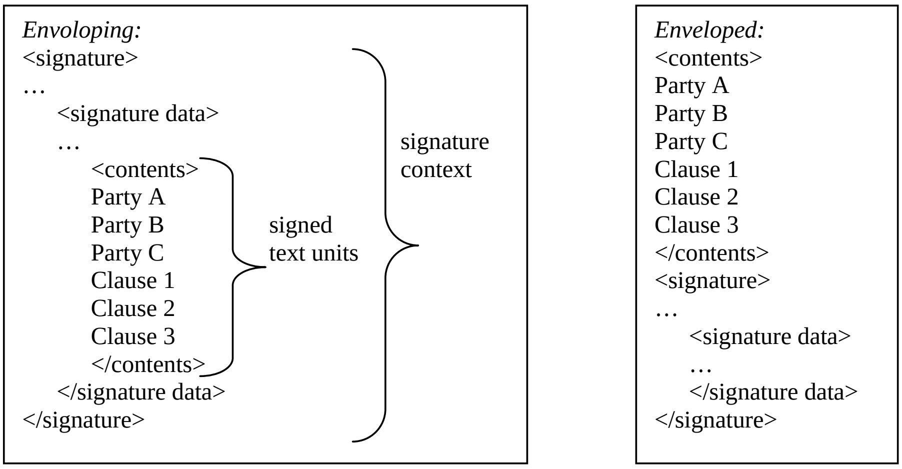

Figure 1: Attached signatures

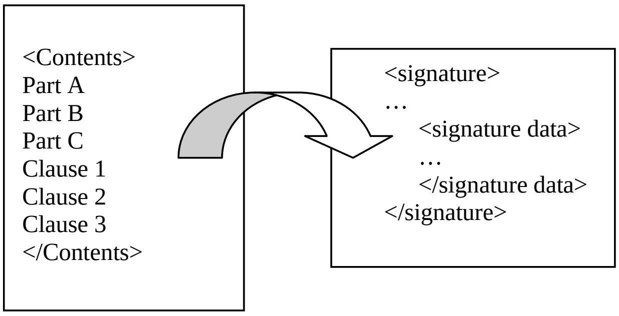

Figure 2: Detached signature

[37] *See* Article 2 (h) of the Data Protection Directive 95/45/EC: 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

[38] A kind of electronic fingerprint calculated mathematically.

6.2 Industry Fora

Borttaget: *Working*

Means and methods for managing electronic signatures do not evolve by themselves and there are industry fora showing a specific interest in these kinds of questions. Emerging legal networks in combination with research and development activities in the field of law and informatics[39] are just a few examples.

Borttaget: working

The network approach can be illustrated by LISA – Legal Information Standards Action Network[40]. It is an international non-commercial network with the overall purpose to support an in-depth understanding of the interaction of law and IT. The LISA network has an open agenda and functions as a supplementary arena for legal review and legal system design beyond formalised representation of legal expertise.[41] LISA focuses not only on system design issues but also on substantive law.

The action plan and goal for LISA can briefly be explained in the following way:

Information standards need to be legally managed
LISA takes responsibility for sharing information about the legal implications of information standards.

The digital network society requires proactive law
LISA plays a new role in the shaping of law in the information market. Major means and methods for LISA are to produce legal reviews of information standards and to contribute to ongoing debates as well as to support legal system design activities.

Trust enhancement is the goal
LISA's overall goal is to enhance legally founded trust in the use of information standards.

Formaterade: Punkter och numrering

[39] The SLIM Project – Secure Legal Information Management – is one example hereof (see further "www.juridicum.su.se/slim/". The Action Plan of SLIM can be summarised in the following focus points: (a) critical analysis of ICT-related security initiatives e.g. XML Digital Signatures, (b) exploring the use of language technology to enhance trust chains in legal information retrieval, and (c) conceptualisation of legal requirements with the prospects of security branding.

[40] *See* further "www.lisan.org".

[41] An umbrella network for the Swedish branch of LEXML (see e.g. "www.lexml.de" which may be described as a European response to the US LegalXML initiative. Formally LegalXML is an OASIS Member Section (Organization for the Advancement of Structured Information Standards) that unites legal and technical experts in a common forum to create standards for the electronic exchange of legal data. There are quite a few technical committees associated to LegalXML: LegalXML Court Filing, LegalXML eContracts, LegalXML eNotary, LegalXML Integrated Justice, LegalXML Lawful Interception, LegalXML Legislative Documents, LegalXML Online Dispute Resolution, and LegalXML Legal Transcripts.

Anyone interested in working with LISA is welcome to join the network as a member or observer![42]

Borttaget: ateur

References

Chiu, Eric, *ebXML Simplified: A Guide to the New Standard for Global E-Commerce*. New York: Wiley, 2002.

Ds 2003:29, *Formel: Formkrav och elektronisk kommunikation*.

Edwards, Lilian and Waelde, Charlotte, *Law & Internet: a framework for electronic commerce*. Second Edition (1997). Oxford: Hart Publishing 2000.

Fejø, Jens, Nielsen, Ruth, and Riis, Thomas, *Legal Aspects of Electronic Commerce*. Copenhagen: Jurist- og Økonomforbundets Forlag, 2001.

ICC comment on the use of advanced electronic signatures by legal persons for security purposes, March 2003, Commission on E-Business, IT and Telecoms Task Force on Security and Authentication, Doc 373-36/4, Paris 2003.

Kronqvist, Stefan, *Brott och digitala bevis: En handledning*. Stockholm: Norstedts juridik, 2002.

Lundblad, Nicklas and Magnusson Sjöberg, Cecilia, *Making Money from Information Standards*. In: XML Europe 2003, 5-8 May, 2003, London, Conference Proceedings. 22 ff. (electronically published on a CD). See also "http://www.lisan. org/li/ docs/ xmleurope/London03/02-05-06.pdf".

Magnusson Sjöberg, Cecilia, *Critical Factors in Legal Document Management*. Stockholm: Jure förlag, 1998.

Magnusson Sjöberg, Cecilia, *Managing Electronic Signatures*. In: EU Electronic Commerce Law. Ruth Nielsen, Søren Sandfeld Jacobsen and Jan Trzaskowski (eds)., p. 95-98. Copenhagen: DJØF Publishing, 2004.

Magnusson Sjöberg, Cecilia, *Tillit i informationssamhället: Kejsarens nya kläder eller förändrade förutsättningar för rättsutvecklingen?* In: Nordisk årsbok i rättsinformatik (NÅR) 2002, Anonymitet Övervakning Tillit p 107-125, Ed. Peter Blume. Stockolm: Jure förlag, 2003.

Magnusson Sjöberg, Cecilia, *Rättsautomation: Särskilt om statsförvaltningens datorisering*. Stockholm: Norstedts juridik, 1992.

Mason, Stephen *Electronic Signatures in Law*, LexisNexis Butterworths, 2003 "http://www.lexisnexis.co.uk/".

Newcomer, Eric, *Understanding Web Services: XML, WSDL, SOAP, and UDDI*. Boston: Addison-Wesley, 2002.

Ramberg, Christina, *Contracting on the Internet: Trends and Challenges*. In: SOU 2002:112 (Swedish Government Official Reports), Law and Information Technology, Swedish Views, An anthology produced by the IT Law Observatory of the Swedish ICT Commission, p. 109-116.

Ray, Erik T., *Learning XML* (Second Edition 2001). Sebastopol: O´Reillly, 2003.

Schartum, Dag Wiese, *Rettssikkerhet og systemutvikling i offentlig forvaltning*. Oslo: Universitetsforlaget, 1993.

[42] Collective positions are drawn up by a formalised procedure of Request for Comments (RFC) and Request for Position (RFP).

Seipel, Peter, *Computing Law: Perspectives on a New Legal Discipline*. Stockholm: LiberFörlag, 1977.

Udsen, Henrik, *Den digitale signatur – ansvarsspørgsmål*. Köpenham: Forlaget: Thomson A/S, 2002.

The Legal and market Aspects of Electronic Signatures Jos Dumortier et.al. Study for the European Commission – DG Information Society, Service Contract Nr. C 28.400. Leuven: Interdisciplinary centre for Law & Information Technology, 2003. Cited: The Legal and Market Aspects of Electronic Signatures, Leuven 2003.

Websites

SAMSET (Samhällets elektroniska tjänster), a Swedish initiative within the area of e-supported public services “www.rsv.se/samset/ samset/html”.

XML W3C Recommendation “www.w3.org/TR/REC-xml”.

XML-Signature Syntax and Processing “www.w3.org/TR/xmldsig-core”.

The SLIM Project – Secure Legal Information Management “www.juridicum.su.se/ slim/”.

LISA – Legal Information Standards Action Network “www.lisan.org”.

LEXML, see e.g. the LEXML network in Germany “http://www.lexml.de/”.

LegalXML, part of the OASIS effort (Organization for the Advancement of Structured Information Standards). Legal XML's mission is to create open, non-proprietary standards for legal documents and applications. “http://www.oasis-open.org/home/ index.php”.