

Trusted Documents

Nicklas Lundblad

Abstract

Trust is emerging as one of the central issues of all communications in the Internet age. How do we evaluate and find that which is trustworthy and discard that which is not? Trust in itself is a fuzzy concept (and therefore an extremely useful one), and the definitions in literature vary from the epigrammatic to the detailed and theoretically dense. The evolution of XML-based vocabularies for e-commerce raises the question of how the trust in these new documents will be ensured. There seems to be an interesting problem here: we trust data in the context of a document. But if we secure the document, the modularity - hailed as one of the great benefits of XML - seems to be lost! And securing the data, the individual tags, makes no sense. We only trust them in context. Either we have trusted and rigid documents, or flexible and non-trusted documents. Is this a necessary conclusion? One possible solution lies in the construction of not a technical protocol, but a legal protocol for handling the transferring of data from documents with conserved measure of trust. The notion of a legal protocol is developed and it is shown that it also would solve some of the as of yet unsolved problems of how to handle personal data in XML-based vocabularies.

This work was carried out in cooperation with FRAMKOM and Stig Berild, in the K-project.

1. Introduction

Trust becomes an evermore important factor in the design of advanced information and communications systems. The notion of trust is inherently fuzzy and the literature presents definitions ranging from the epigrammatic Luhmann-definition (Luhmann 1980): "He who stands by what he has allowed to be known about himself, whether consciously or unconsciously, is worthy of trust." to the theoretically dense

investigations of other researchers (McKnight 1996). The hope of fixating trust in a model is remote. Some researchers pursue more formalistic approaches to trust, with roots in decision and belief logics (Reagle 1996, Josang 1999). Some note the hard to quantify qualities of trust and choose to work with these (Klang 2000). The trust literature is extensive and in most cases it is noted that research in this area, by necessity, is interdisciplinary. The issue of trust can be framed as an issue of cost. What does it cost to search, evaluate and manage trusted relationships? If the answer is that the cost of doing this is less than the expected loss due to fraud or other malicious acts, then the trust evaluation process makes good sense. This interesting since one of the great advantages XML brings is bringing down costs for searching and evaluating information. How can the power of XML be brought to bear on the cluster of trust related problems? There are several ways. In this paper we will review two of them, XML-signatures and S2ML. These reviews will be short and end with some notes on these two initiatives and problems that I think they need to resolve.

2. XML Signature and the concept of legal electronic signatures

XMLSignature offers an interesting and ambitious framework for working with XML and digital signatures. It is a W3C Candidate Recommendation, and expected to reach Recommendation status (or rather: might reach recommendation status) in May 2001 (XML Signatures Syntax and Processing). The idea is to create signatures that can be applied to "any digital content (data object)". Several different and interesting questions can be asked in reference to the initiative, and from a legal viewpoint the first has to be how we work with the recommendation in reference to the European Directive on electronic signatures (Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures Official Journal L 013, 19/01/2000 p. 0012 - 0020 (Hence forward: the directive)).

In what ways do we need to examine the compliance with the directive? On the one hand it seems possible to say that the recommendation is independent of the directive, since it treats ways of "creating and representing digital signatures", while the directive concentrates on the legality and validity of electronic signatures (the

difference between digital and electronic in this case is uncertain, but not crucial). However, there is at least two questions that must be asked of the recommendation. The first is simply this: is the notion and representation of signatures in the recommendation consistent with the definition and concept of electronic signatures in the directive?

The definitions in the directive are laid out in article 2 of the EC-directive. The article is lengthy, but worth quoting in total:

“

the purpose of this Directive: (1) "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication; (2) "advanced electronic signature" means an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable; (3) "signatory" means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents; (4) "signature-creation data" means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature; (5) "signature-creation device" means configured software or hardware used to implement the signature-creation data; (6) "secure-signature-creation device" means a signature-creation device which meets the requirements laid down in Annex III; (7) "signature-verification-data" means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature; (8) "signature-verification device" means configured software or hardware used to implement the signature-verification-data; (9) "certificate" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person; (10) "qualified certificate" means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II; (11) "certification-service-provider" means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures; (12) "electronic-signature-product" means hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the

provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures; (13) "voluntary accreditation" means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification?service?provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification?service?provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

”

Now, is the definition of an electronic signature in the directive consistent with that of the recommendation? There is no stipulatory definition in the recommendation to draw upon in trying to decide this issue, but we can quote a few representative passages in the recommendation and discuss these:

“

XML Signature is a method of associating a key with referenced data; it does not normatively specify how keys are associated with persons or institutions, nor the meaning of the data being referenced or signed. XML Signatures are applied to arbitrary digital content (data objects) via an indirection. Data objects are digested, the resulting value is placed in an element (with other information) and that element is then digested and cryptographically signed.

”

It seems clear that the concept of a digital signature as it is found in the recommendation is slightly from that found in the directive. The directive speaks of electronic data appended to other electronic data for the purposes of authentication. The XML Signature makes no mention of the purpose of signing, and this might be explained by the simple fact that this is a technical recommendation and not legal material. Another, somewhat more palpable difference, emerges when we move on to the second definition in article 2, that of advanced electronic signatures. Is the signature representation in XML-signature the representation of an advanced electronic signature, as this is understood in the directive?

The answer to this has to be no. There are many components missing in the XML-signature. The mention of the signatory in the directive, for example, is not

supported by the recommendation, which makes no mention of the signatory, or the role of the signatory in the process of signing electronically. Especially not of the control parameter implied in Article 2 p. c) above. Yet again this might be explained by the fact that this is a technical recommendation.

But what does this mean? Is this really an important criticism? Yes and no. It might be interesting to be able to represent what the directive refers to as advanced electronic signatures in XML, and of course this signature is by legislators expected to be the signature of choice in the European Union. The adoption of a recommendation that does not encompass these forms of signatures might be considered dubitable. However: it might also be argued that the XML-Signature recommendation doesn't need to comply with the directive in full, this might be accomplished by non-technical means. We might even argue that this should be the case. Technical recommendations should not be overwrought with every possible complication that the field has to offer.

I think, however, that the first view has some important points. A more thorough examination of the concepts in the recommendation and the directive might show that these are too far apart for the recommendation to be used in a meaningful way in the EU-environment. I know that this is pushing it, but the mere possibility should offer pause. I know of no such more thorough evaluation and comparison of the concepts, and my uninformed guess would be that the recommendation has been created with technical concepts of signatures in mind. The societal and legal importance of this technology, however, seems to call for an inventory of legal conceptual space as well. That this is no easy task has been pointed out in the literature (Endersz 1999). It is, however, also well known that a legal strategy for DTD/Schema design is an efficient way of reducing risks and the probability of future unexpected results (Magnusson Sjöberg 1998)

It might also be worthwhile in such a study to include a careful examination of the XML Signature recommendation and points 3 through 13. The conceptual framework outlined by the directive is of lasting importance for businesses that have to comply with these legal concepts rather than those of information security and cryptography science. The framework has also been the object of a few tentative analytical attempts (Reed 2000). Until such an examination has been made, or good reasons presented why it should not be made, the XML-signature remains an interesting but

insufficient tool for the introduction of trusted documents. It should be noted that this conceptual inventory might be a dialogic process! As it has been pointed out new technologies sometimes require us to rethink legal concepts (Seipel 1997).

3. S2ML-is trust seamless?

The other interesting initiative that I am going to discuss in this paper is the S2ML-initiative. According to newly submitted draft 0.8 the initiative deals with authorisation and authentication. The use of the recommendation is outlined in three use case scenarios:

1. User driven transactions
2. Service driven transactions
3. Hosted services

These three are described in some detail in the draft, and I will only summarise them for the purpose of this paper. The first scenario is exemplified in the draft by the user that signs in with a major bank, Then, when moving from the bank to its partners, 401k management firms and brokers et cetera, the user will not be required to log in anew. Instead this will be facilitated by the bank who will pass on the authentication information.

This model is wrought with severe legal problems. I will only mention a few that, from a european standpoint, seems to make the standard entirely impossible to apply. The first problem is related to the collection of personal data. Under the existing directive on dataprotection (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Official Journal L 281 of 23/11/1995) all such collection must abide by a number of rules, among which are consent to the collection of data and some rudimentary requirements on the data collected. There is some discussion today about the use of consent in the data protection the directive, but most parties seem to think that we must allow for implicit consent in certain situations. Logging in on a web site might for example constitute implicit consent that the web logs of the session are collected. But when this

happens seamlessly the whole consent element disappears completely. It is hard to see that this would be acceptable under the rules of the data protection directive.

Another interesting legal problem arises when the newly decided directive on legal aspects relating to electronic commerce is put into effect in the member states (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce")) This directive explicitly confers on all service providers in the information society certain information duties. They have to be clear about their identities, and there must be no uncertainty as to which the service provider is. The customer must know whom he or she is dealing with. Now, with a seamless net like the one sketched above, this might also become a serious problem. If the transferral from one site to another is not clearly stated there seems to be a legal problem here.

Another legal problem is more important: who is responsible for a damage occurring due to the use of transferred authentication? This is far from obvious in the standard, and the liabilities involved should be none to attractive to any party. In short, it is hard to see the applicability of the standard. That this affects the users trust of the web site and the documents therein should be another important factor(Karvonen 1999).

This said, it still would fulfill an important function. The legal framework is not ready for that change, however. How to best address this is a purely political issue.

4. XMI and trust - a fundamental conflict?

One of the great advantages with XML is the ability to mark up data and add semantics to the web. Being able to find interesting pieces of information in a document quickly, extracting them and then using them in applications and for the construction of new documents turns data into modular units that can be used very much like lego, in a sense. When contemplating security issues and issues of trusted documents, however, these enormous advantages of the XML - technology easily turn into disadvantages. The modularity of data is at the core of this conflict.

Consider an arbitrary document containing a set of data $x_1 \dots x_n$. When we trust this document we trust the constellation, arrangement and context of the document and

the data contained therein. We might even refuse to say that we trust the document at all, we might argue that the lowest meaningful level of trust is the entire context of document, data and the situation in which the document exists. When we want to add digital signatures or any other kind of authenticating technology to the document we thus want to conserve as much as possible of the context to preserve trust.

Trust is contextual, and this means that we will require large sets of data to be included in what we might term trusted documents. At the very moment we extract data to use them elsewhere, the status of the data changes from trusted to non-trusted at the same instant the context changes.

This is, of course, wise: consider the case where your name is extracted from an invoice and inserted into a gift certificate. The context changes the meaning of the data. Even though the invoice was trusted, this trust is not transferred with the data to the gift certificate.

The problem can be stated clearly:

We trust only data in context. When they are transferred from one context to another trust inevitably disappears. The great advantage of XML, the ability to mix data and create on-the-fly documents and dynamically change clusters of information, stands against the need for context in trust issues. This dichotomy seems to force us into a trade off: either we keep the dynamic modularity of XML or we keep the trusted documents. We cannot have both. Is this so?

Might it not then be possible to sign the individual data? So that data, when transferred, is transferred with trust? Can we not define a number of contexts into which we allow transfer? (This data can travel with trust constant in between this documents $D_1 \dots D_n$). Of course, this might be possible. I have no doubt that this is solvable by technical means (it might turn out to be a rather difficult problem to define contexts), but I also think that this might be solved by another approach: legal protocols.

With legal protocols I am referring to a simple set of interactions that authorise the transferral of trust in the transferral of data. This is already commonplace in law today. We have rules of denunciation in contract law for example: when a contract is transferred to another party, or when a debt is sold, certain processes for notification

are provided. These processes are easy to implement in digital environments and might very well work out particularly well when it comes to the notification and consent problems I mentioned above in reference to the S2ML initiative.

By defining a set of interactions with the user, or an agent programmed to handle the stream of such requests, the user might condone the transferral of trusted data, and the creation of new trusted documents, by a pre-set of preferences or by acknowledging these transferrals him- or herself. The legal value of the trust in these documents far surpasses the simple technical value of a secure document.

The future might be simpler than we think. There are technical design solutions for many problems, but sometimes there might be more efficient, cheap and workable legal solutions. Sometimes we might just...ask!

Bibliography

[Erdesz, György] Erdesz, György, "Trust Issues in Open Electronic Signature Infrastructures" NordSec 99: Proceedings of the fourth Nordic Workshop on Secure IT systems- Encouraging Co-operation.

[Josang, Audun] Josang, Audun, "Trust-Based Decision Making for Electronic Transactions" in NordSec 99: Proceedings of the fourth Nordic Workshop on Secure IT systems- Encouraging Co-operation.

[Karvonen, Kristina] Karvonen, Kristina, "Creating Trust", NordSec 99: Proceedings of the fourth Nordic Workshop on Secure IT systems- Encouraging Co-operation.

[Klang, Mathias] Klang, Mathias, "Who do You trust? Beyond Encryption, Secure e-business" World Wide Law, BILETA 2000

[Luhmann, Niklas] Luhmann, Niklas, Trust and Power (New York 1980) (transl)

[McKnight, D Harrison] McKnight, D Harrison, "The Meanings of Trust" Working paper MISRC [<http://www.misrc.umn.edu/wpaper/wp96-04.htm>] 1996

[Magnusson Sjöberg, Cecilia] Magnusson Sjöberg, Cecilia, Critical Factors in Legal Document Management (Stockholm 1998)

[Reagle, Joseph M. Jr] Reagle, Joseph M. Jr, "Trust in electronic markets: The Convergence of Cryptographers and Economists" First Monday 1996 (<http://www.firstmonday.dk>)

[Reed, C] Reed, C, "What is a Signature" 2000(3) The Journal of Information, Law and Technology (JILT) <http://elj.warwick.ac.uk/jilt/00-3/reed.html/>

□ S2ML draft 0.8

□ S2ML: The XML Standard for Describing and Sharing Security Services on the Internet (Netegrity White Paper) November 2000

[Seipel, Peter] Seipel, Peter, Juridik och IT: Introduktion till rättsinformatiken (Stockholm 1997)

□ XML Signature Requirements W3C Working Draft 14-October-1999

□ XML Signature Syntax and Processing W3C Recommendation 31 October 2001

Biography

Nicklas **Lundblad**

L.LM, B.A., Ph.D Student
Viktoria Institute/Framkom
Sweden

Nicklas Lundblad - Nicklas Lundblad is working on a PhD in informatics with focus on the cross section in between law and informatics and cognitive philosophy. Is the author of a book and several articles on law in information society and lectures on these subjects.