Fair Digital Signing: The Structural Reliability of Signed Documents

Argyris Arnellos[1], Dimitrios Lekkas[2*], Dimitrios Zissis[2], Thomas Spyrou[2], John Darzentas[2]

[1]Department of Logic and Philosophy of Science,
University of the Basque Country, Donostia – San Sebastian, Spain
[2] Dept. of Product and Systems Design Engineering,
University of the Aegean, Syros GR-84100, Greece
e-mail: argyris.arnellos@ehu.es - {arar; dlek; dzissis; tsp; idarz} @aegean.gr

Abstract

The exchange of digitally signed data inherits all the problems related to the indeterminacy of human communication, which are further intensified by the legal implications of signing. One of the fundamental intrinsic weaknesses of digital signatures is that the signer creates a signature on a series of bits, which may be differently transformed and perceived by the verifier (or relying party), due to the inevitable differences in the intention and the purpose of the two agents. As a result, syntactic and semantic distance is introduced between a signer and a relying party. In this paper we suggest a framework that models the process of digital signing, using several virtual and interrelated levels of communication, thereby promoting the analytic and synthetic exploration of the entities and the transformations involved. Based on this exploration, it is possible to indicate the favourable conditions for mutual understanding between the signer and the relying party. We focus on the syntactic and presentation levels of the communication process and we introduce the notion of structural reliability of a syntactic component, as a measure of how securely and accurately a signed document can be used. It is argued that structural reliability depends on a quantitative metric, such as the structural informativeness along with other qualitative characteristics of the syntactic component. The structural reliability of several document representation protocols is evaluated and it is concluded that the higher the informativeness of the protocol, the less the semantic distance produced, provided that the communicating parties have the capacity to handle this protocol.

Keywords: Security, Fairness, Trust, Digital signature, Structural reliability, Informativeness, Semantic distance, Meaning

1. Introduction

Signing is an action which is always projected in the context of communications between a signer and a verifier. As such, signing is characterized by all the problems related to the indeterminacy of human communication, which are also intensified by legal implications. In the traditional context of hand-written signatures, the signer and the verifier wish to ensure the syntactic integrity of a document, while they both try to agree on a certain state of affairs on the basis of the (diverse) meaning which is expressed by each one within this document.

In the same way, digital signatures fail to avoid the basic problem of misunderstanding, while adding an additional layer of problems due to their computational complexity. Digital signatures are used to preserve the basic security characteristics of digital documents, such as integrity and

[*] Corresponding Author, Tel. +30 22810 97100, e-mail: dlek@aegean.gr

authenticity, while acting as the principal verification method of the signer’s intended meaning, as expressed in the respective document. The creation of a digital signature cannot be denied as an action (non-repudiation), since it can be algorithmically proven, using cryptographic techniques. However, there are many weak points in the procedure of digitally signing data, as due to the inherent computational complexity of the task, it is not performed directly by humans, but only through hardware and software procedures. “Mathematically, it works beautifully. Semantically, it fails miserably. There's nothing in the description above that constitutes signing” (Schneier, 2000). Bruce Schneier a renowned expert in cryptography and computer security commented, “for years, I would explain the mathematics of digital signatures with sentences like: "The signer computes a digital signature of message m by computing m^e mod n." This is complete nonsense. I have digitally signed thousands of electronic documents, and I have never computed m^e mod n in my entire life. My computer makes that calculation. I am not signing anything; my computer is. Due to the nature of this process, several concerns arise, such as who is using the signature-creation-data, whether they are performing a willful act and whether the software and hardware used for this action can be trusted” (Schneier, 2000).

Another important question is whether *the syntactic component* (the signed document in a specific format) is uniformly transformed into a bitmap object, which is subsequently displayed and observed by both the signer and the verifier of the signature (called the ‘Relying Party’ hereinafter), despite the fact that the binary integrity of the communicated syntactic component is guaranteed on the bit level. Communication can be performed at four levels, i.e. the binary, the syntactic, the presentation and the semantic levels, as it will be discussed later. Ambiguities can arise in the interpretation of the data in any of these levels, when this string can be viewed differently by the signer and the verifier of the signature. That is, it is possible to sign a digital document that changes when viewed at a later time, without invalidating the digital signature (Alsaid & Mitchell, 2005). From ancient times steganography has been used to conceal the existence of messages, making use of invisible inks and microdots in such a way that no one, apart from the sender and intended recipient, suspected the existence of a message. In digital steganography, electronic data representations may include steganographic coding inside a document file, image file, or executable program. A binary file may incorporate hidden text or layers not viewable in its final representation, word documents are known to contain “hidden text” text, acrobat files “hidden layers” and image files been embedded in video material (optionally played at slower or faster speed). Therefore, as described in detail in Section 2, one may be held liable for a legally binding digital signature, without in fact having performed a conscious and willful act, due to ambiguities in the transformation and the presentation of the signed data.

As a result, the problem can be described as one of syntactic and semantic distance between signed data, signer’s meaning and relying party’s understanding of this meaning, which is a pure communication security issue. For this definition, *syntactic distance* is at the level of computational transformations and presentation, and *semantic distance* is at the level of human cognition and understanding.

The objective of this paper is to suggest a basic framework for *fair digital signing* that provides a useful model of evaluating signed communication processes and promotes the analytic and synthetic exploration of the entities and the transformations involved. Thus, it is argued that even more favorable conditions for mutual understanding between the signer and the relying party can be supported. This paper enhances previous research done in this direction, which focused on exploring the syntactic and semantic differences introduced by digital signatures, in the context of electronic commerce communications. Prior work concluded that the document syntaxes based on markup languages (XML and HTML) or plain bitmap images were highly preferred for applying and verifying digital signatures in e-commerce applications, as they presented the preferred solution with the lowest informativeness (informativeness being a measure of the probability of occurrence of the symbols within the document), highest human readability on the syntactic and the semantic level, and high redundancy (Arnellos, Lekkas, Spyrou, & Darzentas, 2005). This present paper adds to the given body of knowledge in the field, while enhancing previous research and adding the theoretical framework for *fair digital signing*, that provides a useful model for evaluating signed communication processes in a wider context.

In contrary but also in complement to Arnellos et al. 2005, this work emphasizes on the inevitability of the introduction of the semantic distance between signer and relying party, on the detailed introduction of a model depicting the different levels of communication and transformation during the action of digital signing together with a schema mapping the wider framework's components and their interrelationships. Particularly, in this work, under the perspective of fair digital signing and of the proposed framework that aims in maximizing understanding together with reliability the main objective is to reduce the semantic distance, providing the involved parties with favourable conditions for mutual understanding. We focus on minimizing the semantic distance between interacting parties and it is argued that, in the case that no noise is introduced in the syntactic and presentation level, the most structurally reliable syntactic component will be the one which will use the formatting protocol with the highest informativeness, as long as it is equal or lower than the semantic (representational) variety of the involved parties. The qualitative evaluation of the structural integrity of a syntactic component is based on several new parameters and a detailed discussion and a mathematical proof showing the behavior of informativeness after the insertion of new symbols into a document is included, leading to some very useful conclusions.

In section 2 we examine the process of signing and assigning meaning to a document and how effectively this process is digitally translated. We identify a number of weaknesses introduced through the digital translation of this process and go on to show how these weaknesses relate to the amplification of the semantic distance in communication. As we shall discuss in Section 3, the introduction of a semantic distance between the signer and the relying party is inevitable. An indicative characteristic of this framework is that the semantic distance is related to the *communication reliability* of the syntactic component, which can be considered as the combination of its *structural* and *lexical content reliability*. In order to explore this in detail, Section 4 examines the level of structural reliability of a signed document. In particular, the several formatting transformation protocols that can be selected and applied on the binary component will result in a syntactic component and subsequently in a respective component in bitmap format. Considering that this format affects the structural reliability of the syntactic component, we explore how the structural characteristics of the syntactic component might be related to the semantics that the signer or the relying party will produce by their interaction with it. We posit the relationship between the structural characteristics that are provided by a formatting transformation protocol with the *structural informativeness* of the respective protocol. We show how the structural informativeness of several well-known formatting protocols (XML, HTML, PostScript, Bitmap, PlainText, etc.) may be quantitatively measured, providing an indication of their possible structural capacity to inform. This metric is related to the structural variety (richness) of the syntactic component which, in order to be deemed as structurally reliable in the context of fair digital signing, it should be compatible with the semantic variety of both the signer and the relying party.

Finally it is shown that some of the characteristics described that increase the redundancy of a syntactic component (e.g. the existence of meta-data and the embedding of transformation protocols) are directly connected to the value of informativeness. Since they increase the number of symbols used, they generally increase the informativeness of the document. However, this holds only until a threshold in the appearance frequency of the new symbols is reached.

2. The Action of Signing and its Intrinsic Weaknesses

Signing is a personal act, which is validated and taken under consideration in the context of communications between a signer and a relying party. Generally speaking, when two people wish to agree on a certain state of affairs, they firstly each communicate their point of view regarding this state of affairs. An individual's point of view, is perceived as the individual's meaning assigned to a specific state of affairs. Subsequently, capturing this conceptual meaning and expressing it within a document, which can be verified or validated through the application of a signature on the document, is the essence of the act of signing. Hence, a signature evidences the signer's meaning with respect to the document signed. The nature of the signer's meaning will vary according to the transaction, and in all cases could be better approached, but never fully determined, only by looking at the context in which the signature has been created. A signature, may signify, for example, liability against an obligation, legal binding to the terms of a contract, the approval of a third party's request, authorization to transfer funds, confirmation that the signer has read and reviewed the contents of a memo, an indication that the signer was the author of a document, or merely that the contents of a document have been shown to the signer and that she has had an opportunity to review them. In all these cases, the signers verify their meaning as it is captured in the documents, which are then used in each context. The signer, by applying a signature, as confirmation of meaning, is simultaneously accepting the probable penalization of the actions taken based on this meaning. Thus, a signature is often used to satisfy legal obligations or regulations that require the presence of a signature before a document can be considered legally effective. In European law, the electronic signatures directive (1999/93/EC) and other national laws, grant digital signatures the legal validity equivalent to traditional hand-written signatures, electronically emulating a legally binding *signing* act. The application of a signature is an action with great legal validity and any alteration on the structure of a signed document, renders the signature - and consequently any legal implications of the signed document - completely invalid.

The creation and verification of digital signatures, is based on public key cryptography, where the signer encrypts (signs) a sequence of data using a private key and the verifier of the signature ensures the originality of the data by decrypting the signature using the public key of the signer and obtaining the original data (Rivest, Shamir & Adleman). Public key cryptography has reached a stage of relative maturity, due to the intense scrutiny and research that has occurred in this area over the past two decades, currently incorporating many value added characteristics into the signing process; hash algorithms have given a solution to the computational efficiency of the signatures, digital certificates (Cooper, Santesson, Farrell, Boeyen, Housley &Polk, 2008; Kohnfelder, 1978) and self-certified keys (Girault, 1991) provide the means for effective identification of the signer, Public Key Infrastructure (PKI) architectures built the necessary trust relationships and finally time-stamping and notarization techniques provide additional proofs that add value and longevity to a digital signature (Adams, Cain, Pinkas, Zuccherato, 2001; Lekkas, Gritzalis, 2004).

A fundamental intrinsic problem of digital signatures (Maurer, 2003) is that the action of their creation (i.e. the display of a digital document and the usage of a private key) is not directly bound to a physical entity, but only indirectly through a machine and an application. The implicit risk lies in the fact that the calculation of a digital signature is performed transparently by hardware and software (the signature-creation-device) that is mostly unknown and non-trusted by the end-user and potentially may be maliciously corrupted or at least unreliable. The problem is that while a digital signature authenticates a document up to the point of the signing computer, it doesn't authenticate the link between that computer and the signer. An effective example being the process followed when digitally signing an email using PGP (Pretty Good Privacy): an email security program which digitally signs emails). When applying a digital signature to an email, a passphrase is requested and then the digital signature is calculated and appended to an email. "Whether I like it or not, it is a complete article of faith on my part that PGP calculates a valid digital signature. Someone could easily write a rogue version of the program that displays one message on the screen and signs another. Someone could write a Back Orifice plug-in that captures my private key and signs documents without my consent or knowledge" (Schneier, 2000). There have already been reports of computer viruses that attempt to steal PGP private keys. The mathematics of cryptography, no matter how strong, cannot bridge the gap between a signer and his computer, because the computer is not trusted. Technically speaking, a digital signature is applied to a string of bits, whereas humans and applications "believe" that they sign the semantic interpretation of those bits. The problem is that the semantic interpretation of bits can change as a function of the processes used to transform the bits into semantic content. It is relatively easy to change the interpretation of a digital document by implementing changes on the computer system where the document is being processed. From a semantic perspective this creates uncertainty about what exactly has been signed. Risks may be identified in both the proper usage of the private key and the objective notification to the signer of what exactly she is signing, known also as the issue of 'What You See is What You Sign' (Josang et al. 2002). Josang et al. showed how font substitution can be used to display the same digital document with different meanings on different computers (Josang et al. 2002). However, the creator may embed dynamic content, e.g. macros or JavaScript, in a document to change its displayed contents when viewed after the signature has been applied. Kain et al. (Kain et al. 2002) described the problem and gave some examples of applying Time/Date-Based Attacks, Macro-Based Attacks, Linked file Attacks, Platform-Based Attacks, Event-Based Attacks on MS Word, MS Excel, PDF, as well as HTML documents altering their content without invalidating the digital signature. As a result, one may be held liable for a signature created by his private key on arbitrary data, without having full awareness or consent on this action.

XML Signatures have been proposed as solutions to protect the integrity and origin of a variety of document types. One important property of XML Signature is that signed XML elements along with the associated signature may be copied from one document into another while retaining the ability to verify the signature. This can be useful in scenarios where multiple actors cooperate, process and potentially transform a document throughout a business process. However, this same property can be exploited by an adversary, allowing the undetected modification of documents (McIntosh & Austel, 2005). Altering the location of an element within a document can severely impact its semantic meaning.

In practice, there is a fundamental conflict between modern systems (including operating systems, applications and user interfaces) and security (in terms of protecting a secret key and securely presenting to the user what is being signed) due to the increased systems complexity and reduced transparency. Hence the problem. Essentially, there is no means to prove that the signature creator is performing a conscious and willful act when applying a digital signature to a given dataset. This fact is the basic weakness of digital signatures compared to the hand-written signatures – which although they are easy to forge, sometimes not-recognizable and are not securely bound to a person's identity – their creation is under the direct control of the signer and directly bound to the signatory material (e.g. a piece of paper), that has a much more straightforward representation than its binary counterpart.

Summarising, the major weakness of digital signatures within this context is that they are not directly controlled by the signer, since:

- A D. Signature is created by various APIs, interfaces and subsystems, not necessarily trusted, while it is almost infeasible for a signer to control the procedure by creating or verifying a digital signature by hand.
- A D. Signature is calculated on binary data that may be differently interpreted and represented when creating a signature or when verifying a previously generated signature.

In the following section we show how these weaknesses relate to the amplification of the semantic distance in communication and how they can be mitigated by better controlling some parts of the digitally signed communication process.

3. A Framework Describing the Intentional Action of Digital Signing

In this section, we attempt to define a theoretic framework encompassing the main concepts involved during the process of digital signing. Within this framework, the action of signing is considered as a purposeful action, and as such it can be widely considered as cognitive agent-oriented. Thus, we start by describing the cognitive process and we try to indicate concepts which are deemed as relevant for our problem at hand. The basic concepts of the framework include the notions of cognition, intention, meaning, and communication, in the semantic, presentation and syntactic levels as well as the distance observed at these levels. The main objective of the proposed framework is to explore different ways of controlling and possibly reducing these distances.

Figure 1 presents an abstract representation of the communication process between signer and relying party and the semantic distance between them. More specific levels of communication will be suggested and presented in the proposed framework and their reasoning will be discussed.

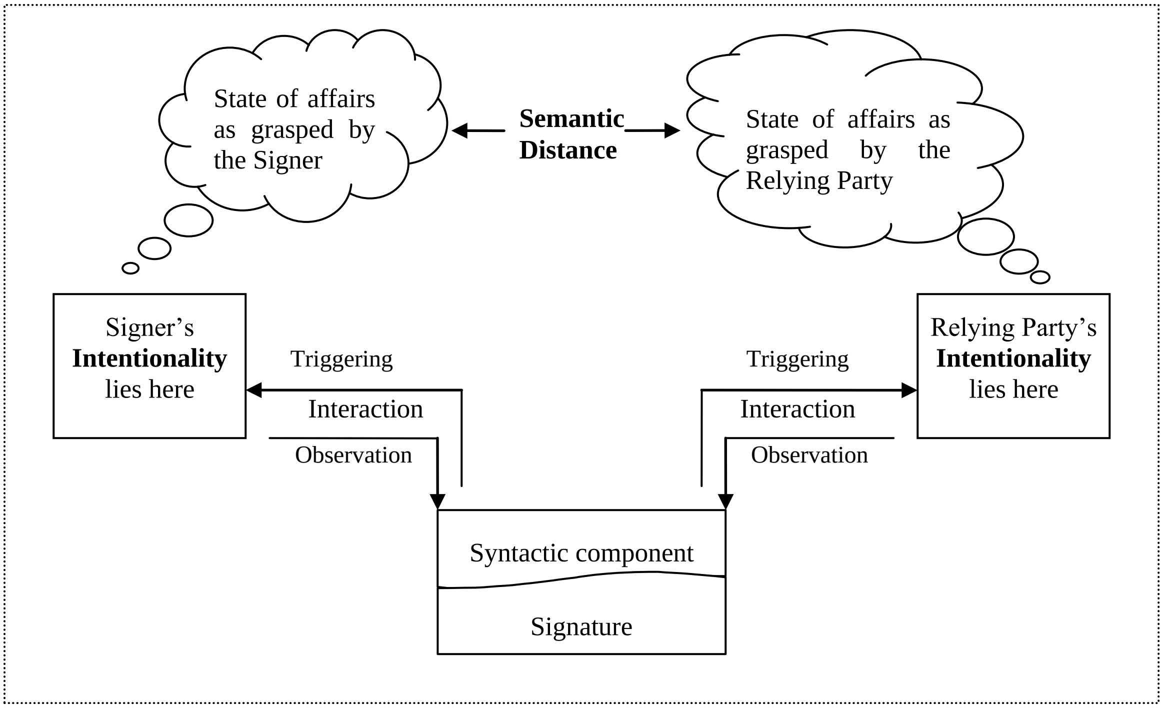
State of affairs as grasped by the Signer
Semantic Distance
State of affairs as grasped by the Relying Party
Signer's Intentionality lies here
Triggering
Interaction
Observation
Triggering
Interaction
Observation
Relying Party's Intentionality lies here
Syntactic component
Signature

Figure 1: *Semantic distance between signer and relying party*

Based on the discussion of these entities of the framework, we will explore the relation between the structural reliability of the syntactic components, and the semantic distance in digitally signed communications.

Cognition is related to the behaviour of agents or rather, aspects of their behaviour that are usually classed as purposeful. The ability of cognitive agents to engage in purposeful interaction with their environment is called *intentionality*. Meaning (representational content) and information are widely considered as the main constituents of cognition. We argue that these properties should be discussed and included in the rationale of the design and presentation of the proposed framework, as they provide a new perspective and understanding of the nature of the signing process. This will help us improve the communications between a signer and a relying party, by providing conditions to reduce the respective semantic distance.

3.1 The Semantic Distance between Signer's Meaning and Relying Party's Understanding

From a cognitivistic or rationalistic perspective, agent and environment are considered as two separate systems. The environment, consists of an objective reality, made up of well-described state of affairs, bearing properties and entering into relations which are governed by their own laws. The cognitive agent is preoccupied with knowledge in the form of representations that are part of the agent's mental states and a cognitive action is characterised in terms of relations among these representations and between them and the environment. Therefore, cognitivism suggests that the mental states of an agent have a content in terms of representations that carry objective information about certain states of affairs in the world. In that case, *the intentionality of an agent is the sequential sum up of all its representations* (Christensen & Hooker, 2004).

On the other edge of the philosophical approaches to the theory of mind is the phenomenological school, which studies the mind in terms of its experiences and its actions (Heidegger, 1962), (Merleau-Ponty, 1962). In this perspective agent and environment are considered as a single system and meaning is an emergent and not a predefined property, described only in the context of the intentional behavior of the whole agent in its environment. The meaning used by such an agent is not as concrete and easily manipulated, as in the cognitivist approach. Particularly, we could speak of meaning as a functional property of an agent that carries relevant and subjective information about the agent's interaction with the environment. In this case, *information acquires a representational structure only in the context of an intentional action* (Christensen et al, 2004). In the rest of the section we argue that in the intentional action of digital signing the semantic distance between the signer and the relying party is inevitable.

Whether from the rationalist or the phenomenological point of view, it may be implied that a signer is, at any moment, in a certain functional state. That state results from the signer's history of interactions with her environment. Whatever the structural type of such a state, it can play the role of a representation. In the context of this paper, we are not concerned about the exact nature of these representations. It suffices to consider that they are used by the signer in order to relate to a distal state of affairs. A representation is connected to the signer's world in terms of what its content is about. The content of the representations is the signer's subjective information about these states of affairs. It is not a mere description of them, but a rich and complex representational structure indicating the type of relation (e.g. belief, desire, hope, fear, etc.) and the possible ways such a relation between the specific signer and its respective states of affairs could be achieved. Furthermore, it seems that for these meaning structures to play a role in the signer's interaction with the respective state of affairs, some kind of triggering that will select them (in the most general way) should take place. This triggering is somehow related (although not absolutely necessary) with the respective state of affairs that perturbs the signer's cognitive capabilities, resulting in information, that is, the formation of new meaning.

Since we consider the signer to be a cognitive agent the signer has an intentional attitude providing her with a meaning towards a certain state of affairs (She takes this meaning as information regarding that state of affairs and wishes to communicate it to the relying party, so that the latter be aware of the signer's meaning and therefore, about her intentionality towards this state of affairs. The signer creates or reads a *syntactic component* (e.g. legal document in a certain format), in which she tries to express this meaning. Then, she is carefully interacting with (observing) the syntactic component (through its analogue - bitmap representation) to see if it clearly (to a degree defined differently by each signer) expresses her meanings, that is, the way she relates her cognitive state with the respective state of affairs. If the signer is satisfied with this expression, and wants to certify that this syntactic component can be used to provide her own meaning (understanding) about that state of affairs, she signs the document.

At this point some very important issues need to be noted.

- First of all, the signer signs her meaning and this is expressed with the syntactic component but not the syntactic component itself.
- Since the signer has some intentionality regarding this state of affairs, it has a meaning for it, and thus, she is able to inform someone else about it.
- The syntactic component never carries any meaning by itself. It is the tool that is used as a trigger from the representational structure of the signer, which creates a meaning in her for that state of affairs.
- If the signer finds this meaning in accordance with her intentionality towards this state of affairs, she concludes that the syntactic component is reliable.
- She then believes, given the fact that she wants to communicate this meaning and given that she shares the same (agreed) collection of symbols (alphabet) and rules of their arrangement (syntax) with the relying party, that this syntactic component is able to inform the relying party in a respective manner.

Therefore, despite the similarity (within a well-specified range of values) of the material foundation (substance/hypostasis) between the signer and the relying party, the same triggers (syntactic components) will not result in the same information. Assuring only the structural integrity of the syntactic component will not necessarily result in reliable communications.

Therefore, *the semantic distance between the signer and the relying party is inevitable* and it should be presupposed in any application of a digital signature.

3.2 Analysis of the Proposed Framework

The previously mentioned semantic distance, which is inevitably introduced during the signatory process, presents a crucial miscommunication problem between communicating entities and a concealed security problem. The proposed framework towards fair digital signing provides a useful model of signed communication processes and promotes the analytic and synthetic exploration of the entities and the transformations involved. Thus, it is argued that even more favorable conditions for mutual understanding between the signer and the relying party are supported. It presents a practical support tool for IS architects, designers and researchers, to understanding the ambiguities and complexities which are inevitably introduced during the signatory process. This framework attempts to shed light on these unavoidable perplexities and provide a support tool for the selection of protocols with the ability to reduce these difficulties. This research concludes on proposing recommendations of considerations that can assist in achieving better communications. A major suggestion of the proposed framework is that it is deemed necessary to model and analyze all communications between the signer and the relying party, prior to initiating any interactions, at the specified four levels of communications (the semantic, presentation, syntactic and binary levels) i.e. the communications at the *semantic*, the *presentation*, the *syntactic*, and the *binary*, levels. Also, the transformation processes between these levels are introduced (figure 2).

The true path of communication (denoted by solid lines) traverses all the abovementioned levels on both sides.

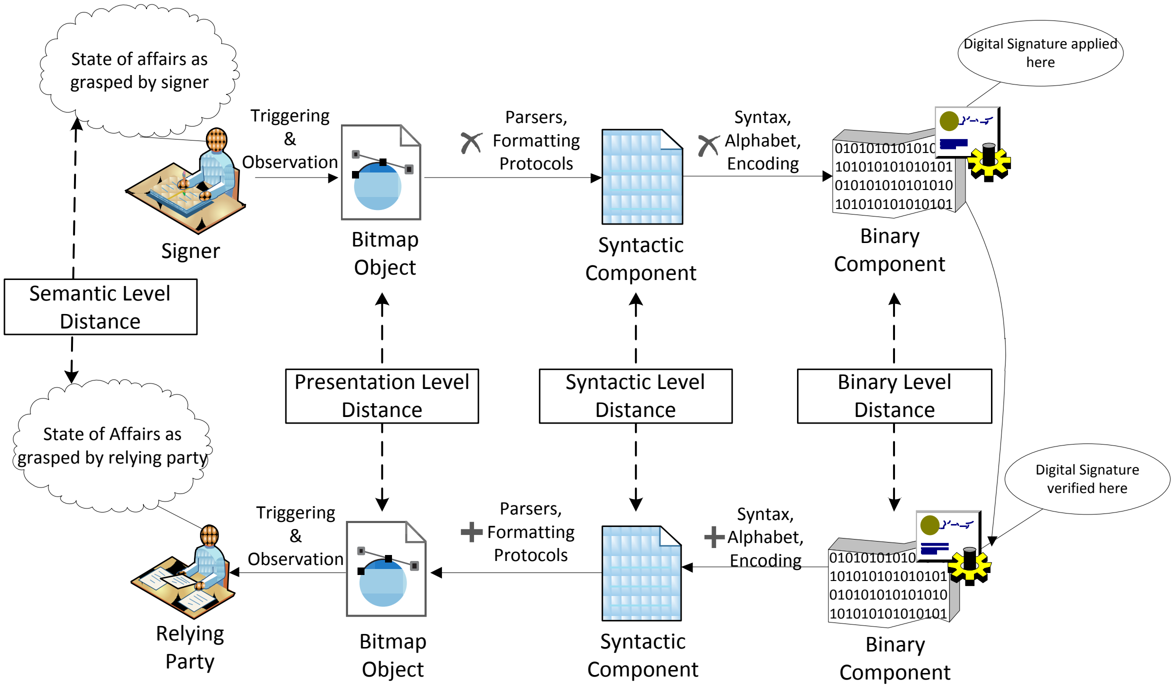

Figure 2: *Diagrammatic presentation of the model depicting the levels of communication during the intentional action of digital signing*.

As illustrated in Figure 2, following the path from the signer to the binary component, the assumed highest level is the *semantic level*, at which, as analysed in section 3.1, the meaning which corresponds to the signer's intentionality towards a certain state of affairs is what he/she wishes to communicate to the relying party.

The signer attempts to translate the states of affairs as he/she has perceived them, into an accurate bitmap representation. The presentation level is deemed necessary to support the interactions between the signer and the bitmap object and consequently the syntactic component. Therefore, these two levels (*presentation and syntactic)* are very crucial. The main transformation is the one that corresponds to the signer's interaction with the bitmap object (*presentation level*). During this interaction, the signer attempts to express her meaning into the bitmap object which may result in the decision (acceptance or rejection) of the signer to apply a DS to the syntactic component, by means of the mental process abstractly described in section 3.1. This level of communication emerges from the signer's interaction directly with the bitmap object and consequently with the syntactic and binary components. Therefore, on the signer's side the syntactic component is created from the transformation of the captured bitmap object by means of certain parsers and formatting protocols. The syntactic component which is used as a trigger for the semantic level of the two communicating parties, becomes a well-formed structure based on known formats such as HTML or PostScript. These structures are produced by means of various syntactic rules (alphabet, syntax, encoding, etc.) of computational nature, resulting in the formatted syntactic component. In the case of the traditional hand-written signature this corresponds to the level where the signature is applied. It should be noted that the fact of a communicated misinterpretation (existence of semantic distance) is the result of a somehow predetermined and pre-agreed correspondence between the components that consist the syntactic structure (i.e. a microstate of the semantic level) together with a non-predetermined selection of one of their possible combinations (the macrostate of the semantic level). The importance of the distinction between those two dimensions of the semantic level is analyzed in Section 4.

In the case of digital signing the introduction of the next level which is the *binary* one is imperative in order to support the transmission of the signed syntactic component. It should be noted that the process of applying a digital signature, is performed at a binary level. The result is a series of bits computed on the binary component, neglecting the series of possible transformations performed until their interaction with the signer. The algorithmic validation of a digital signature also takes place at a binary level, where cryptographic technologies guarantee to a large extent the integrity of data (Rivest, Shamir & Adleman, 1978).

On the side of the relying party the signature is algorithmically verified against the signed binary representation of the formatted syntactic component, together with some additional inspections such as the validity of the certificate of the signer, and the timestamp of the signature (Adams et al, 2001). Then, the binary component would be similarly (accordingly) transformed, by means of certain parsers and formatting protocols to the syntactic, presentation, and semantic levels, to the meaning grasped by the relying party.

As has been discussed above, the distance at the binary level can almost be eliminated, although there may be some problems of technical nature (Lekkas, Arnellos, Spyrou & Darzentas, 2005) which are not considered in the present study. Also, it should be noted that in order for the transition from the binary to the syntactic level to take place, the two communicating parties should have a priori agreed upon the syntactic rules that will be applied at the syntactic level. Hence, the respective syntactic distance (see Figure 2) could additionally be introduced in case of different usage of the syntactic rules.

In general, the application, validation, and verification of the digital signature are performed only at the binary level, while all other levels are not taken into account. Hence, there is an apparent differentiation causing a small degree of independence between the binary, the syntactic and the presentation levels. Although there is a correspondence between the bit sequences in the binary level, the symbols together with their interrelationships in the syntactic level, and the respective analogue object in the presentation level, the validation of the signed syntactic component takes place only on the binary level. Consequently, the action of the creation or validation of a digital signature, that is, the display of a digital document and the usage of a private key, which happens, in as far as it concerns the signer or the relying party, at the syntactic and presentation level, is not directly bound to a physical entity (functioning at the binary level), but only indirectly through a machine and an application. The digital signature essentially only assures the integrity of the binary component (i.e. the two communicating parties share the same binary data) while it does not provide any assurance that the two parties transform identically the binary data on the syntactic and the semantic levels. In other words, it is the ambiguities of the transformation protocols and parsers used to transform the syntactic component into a bitmap object that introduces the respective distances in the syntactic and presentation levels.

Therefore, without considering any possible problems of technical nature at the binary level and at the coding transformation from the binary to the syntactic level, as well as disregarding any possible noise that may exist in the analog channel between each communicating party and the presentation level (i.e. assuming that there is no loss of integrity due to any reason caused by physical means or human inabilities), we focus on the cumulatively added distances on both sides of the communication, on both the syntactic and the presentation levels, which in turn affect the semantic distance. Specifically, *aiming at a fair digital signing, we attempt to argue on how this semantic distance can be mitigated*.

Throughout the proposed framework a number of terms are used. Within the context of this paper we refer to:

- ‘Semantic distance’ as the difference in understanding between interacting parties (human cognitive level).
- ‘Binary component’ as a binary collection of symbols.

- ‘Syntactic component’ as a binary component and syntactic rules (alphabet, syntax, encoding, etc). A well-formed structure based on known formats such as HTML or PostScript.
- ‘Syntactic distance’ as the computational distance.
- ‘Semantic variety’ as the set of different understandings one may exhibit when interacting with components of a particular syntax.
- ‘Syntactic variety’ as the set of different combinations a certain syntax can support.
- ‘Informativeness’ as a measure of the probability of occurrence of the symbols within the document.

Briefly stepping through the proposed framework provides us with the bellow schema mapping the framework’s components and their interrelationships:

1. ***Semantic distance*** is related to the communication reliability of the ***syntactic component***.
2. ***Communication reliability*** is related to the ***structural*** and ***lexical content reliability***.
3. The ***format*** of the ***syntactic component*** affects its ***structural reliability***.
4. We explore how the ***structural characteristics*** of the ***syntactic component*** are related to the ***semantics*** of the two participants in the communication.
5. We continue by defining the relationships between ***the structural characteristics provided by a transformation protocol*** and the ***structural informativeness*** of the respective protocol.
6. The ***structural informativeness*** of several protocols is ***quantitatively measured,*** providing an indication of their possible structural capacity to inform.
7. The metric is related to the ***structural variety (richness)*** of the ***syntactic component***.
8. ***Structural variety*** should be compatible with the ***semantic variety*** of both parties.
9. Other properties that cannot be directly measured (quantitatively) are also discussed and related to the metric of ***informativeness***.
10. Conclusively, we argue that to reduce the semantic distance between communicating parties the formatting protocol must be chosen that has the the highest informativeness, as long as it is equal or lower than the semantic (representational) variety of the involved parties (i.e. highest informativeness<=semantic variety).

3.3 Reducing the Semantic Distance in the Context of Fair Digital Signing

Considering that the agents engaged in digital signing acknowledge any legal repercussions of the actions (decisions) they have made based on the meaning they have exchanged, the overall aim is to support fair digital signing, which is the semantic co-ordination of the signer and the relying party. Hence, the objective is to reduce as much as possible the given semantic distance between the signer and the relying party. This provides with even more favourable conditions for mutual understanding, and thus further strengthens the trust within the signing process.

Under the proposed framework’s perspective, the common tool used for this co-ordination (i.e. the syntactic component), should have the property to reliably affect each part in terms of the respective state of affairs. Therefore, the functional significance of the signature is twofold, that is at the syntactic level (structural reliability/integrity of the syntactic component), and at the semantic level where, as we have seen, a subjective verification of meaning is taking place. Based on the present framework, the problems at the semantic level are very important as the signer and the relying party could have verified their agreement on a state of affairs that in reality they disagree upon.

The problem is concentrated in the *communication reliability* of the syntactic component, which in this specific case, can be rendered into two different but interrelated dimensions: (A and B)

A. in the *structural reliability* of the syntactic component during its interaction with either parties, in terms of:

> *A1.* the structural characteristics of the syntactic component with respect to its ability to convey the signer's choices to the relying party in a way compatible with the ability of both parties to intentionally interact with these characteristics. In this case it is postulated that there will be no transformation ambiguities in the structure of the syntactic component (zero distance (noise) at the syntactic and presentation level – see Figure 2).
>
> *A2.* the structural ability of the syntactic component to compensate for the possible loss of its integrity. It should be noted that in this case, the structural integrity of the syntactic component is at stake, while the integrity of the binary data (binary component) is secured by the digital signature. Hence, it is postulated that the structure of the syntactic component would be differently transformed (introduction of distance (noise) at the syntactic and presentation level – see Figure 2).

B. in the *lexical content reliability* of the syntactic component, that is, its ability to objectify, as much as possible, the semantics emerged through its interaction with either parties. This is a problem of a linguistic nature related to any kind of communication between two or more cognitive agents and it is especially related to the selection and organisation of the lexical content that will be used in the syntactic component.

There is a specific distinction between dimension *A* and dimension *B*. The latter is directly related to the selection and combination of the lexical content of the syntactic component and the semantic ambiguity that is respectively introduced, while dimension A concerns aspects of the transmission of the syntactic component after its creation and simultaneous interpretation by the signer as well as during but also before its interaction with the relying party at the presentation level. We must note that in the scope of an intentional interaction of a cognitive agent with a syntactic component, dimensions *A* and *B* are interrelated. However, the detailed examination of dimension *B* is out of the scope of this paper, as a general and wider aspect of human communication.

In the following sections we will focus on dimension *A* and we will analyze the aspects related to the *structural reliability* of a *syntactic component* that will in turn affect the *total communication reliability*.

3.4 The Structural Reliability of the Syntactic Component in the Context of Fair Digital Signing

We have so far seen that in the proposed framework, the signed syntactic component is the tool based on which the signer and the relying party will communicate regarding a certain state of affairs. We can safely assume that the signer and the relying party are sharing an agreed collection of symbols (alphabet) and syntax. Given that they both want to be co-ordinated with respect to a certain state of affairs, in spite of the semantic distance which is taken as given (the indeterminacy of communication), we could presume that the greater the structural similarity of the syntactic component (as this is transformed into a bitmap object) with which they interact, the closer the constructed semantics regarding this state of affairs. Yet, we recognise that no such completely unambiguous syntactic component exists. Moreover, even if such a component were to exist, its respective binary component could be differently transformed into a different bitmap object (both in the part of the signer and the relying party) disregarding the rules of the respective formatting protocol. In this case, the structural integrity of the resulting formatted and signed syntactic component would be damaged, increasing each party's subjectivity and consequently their semantic distance. Such cases as those of false positives, false negatives (Lekkas et al, 2005) and many others belong to the dimension *A2* of problems regarding the structural reliability of the syntactic component.

In cases where the structural integrity of the syntactic component cannot be compromised, thus, considering a zero distance at the syntactic level (dimension *A1*), one would expect the communication reliability of the syntactic component to be the highest possible. This is not so. Under the perspective of a fair digital signing, in spite of these extremely favorable conditions, the communication reliability cannot be deemed as the highest possible, *unless it is assured that the signer and the relying party are able to fully exploit the syntactic component*. A useful cognitive metaphor, to help with the understanding of such a principle, is the example of a cryptographic expert attempting to describe to a student the principles of public cryptography. Although both entities share a common language (keys, signing, etc.), a different conception of principles leads to a lack of communication efficiency. In general, it is not enough for the two parties to interact with the same syntactic component, but both parties should be able to handle the complexity of the syntactic component and hence, they should have the prior knowledge in order to be able to use all its characteristics. In such a case, it could be argued that the conditions under which the application and the acceptance of a digital signing takes place, are equivalent for both parties. They initiate their interaction with the syntactic component from an equal base as far as that is possible, therefore, they have an as much as possible equal chance to intentionally interacting with it in order to achieve the best possible co-ordination towards a common state of affairs. The reduction of the semantic distance is considered as the greatest possible and therefore it could be argued that these are the required conditions to achieve fair digital signing. On the other hand, if at least one of the involved parties does not have the prior knowledge to be able to fully use the syntactic component, their resulting co-ordination will not be the best possible, hence the reduction of the semantic distance will not be as great as it could be. It can be safely argued that these are not the best conditions towards a fair digital signing.

In order to infer towards this direction regarding cases belonging to dimension *A1*, what has to be made certain is the suitability of the structural characteristics of the syntactic component to be used by both the signer and the relying party. Specifically, what should be located/identified are the characteristics (properties) of the structure of a syntactic component related with the creation of meaning in either parties. In the literature, so far, there are many attempts to map the correspondence between the syntactic and the semantic realm, as well as to measure the amount of semantic information (meaning) that a syntactic component may convey (see for instance Bar-Hillel & Carnap, 1964, Zeevat, 2002 and Rapaport, 1995, 2002). However, these endeavours and the resulting theories bear a lot of problems that make their application unrealistic and impractical for real-world situations (see Mingers, 1997, Floridi, 2004b and Greenberg and Harman, 2006 for related analysis) as these that happen in the domain of digital signing.

Therefore, it seems that the main obstacle in the present attempt is that *there can be no direct and measurable connection* between a syntactic component interacting with a cognitive agent and the general semantics constructed by her. Focusing on the fact that the transformational procedures based on the selected formatting protocol affect the resulting structure (format) of a syntactic component, what should be done is to find the way these structural characteristics of the syntactic component are related to the possible quantity of information that can be created by the cognitive agent. This will give us the opportunity to better infer towards their suitability regarding their usage by either party. In the next section, Shannon's information theory is used as a tool to measure some important structural characteristics.

4. Structural Informativeness of a Syntactic Component

In information theory, *entropy* is the measure of uncertainty associated with a random variable. The term usually refers to the *Shannon entropy*, which quantifies the expected value of the information contained in a message, usually in units such as bits. In Shannon's Mathematical Theory of Communication (Shannon & Weaver, 1998), the information conveyed in a message (a syntactic component in the context of digital signing) is inversely related to the probability of occurrence of this message, or the unexpectedness of the receiver regarding that message.

Within this context information can only be defined when there is both a sender and a receiver. However, it doesn't deal at all with the semantic aspect between them, that is, the meaning that a message may raise in the sender or the receiver. On the contrary, it is a purely quantitative approach to the definition of correctly transferring, as much as possible symbols, in an as fast as possible rate, from the sender to the receiver, via a given communication channel. Thus, the amount of units of information produced by a sender *S* communicating a message *M* from a set of messages consisting of *N* equiprobable messages, equals the number *H* of binary decisions needed in order to select a particular message from them. Formally, we may say that

$$H=log_2N \qquad \textit{eq. 1}$$

In this case, the prior probability of occurrence of each of the *N* messages is equal to $P=1/N$. Thus, based on the additive property of the quantitative measure of *H*, we can say that the information content I_i of the i^{th} message of a source *S*, with prior probability P_i and $\sum_{i=1}^{N} P_i = 1$ is given by the equation:

$$I_i = -log_2Pi \qquad \textit{eq. 2}$$

Hence, in this framework, the lower the prior probability of occurrence of a message, the higher is the information content of its occurrence. The quantity I_i provides the novelty value of the specific message (Küppers, 1990).

We can now generalise that for a binary source producing messages consisting of *N* symbols with prior probabilities of occurrence $\{P_1, \dots, P_n\}$, where $\Sigma P_i = 1$, the average informativeness, that is, the average information or the expectation value of the information content, of a message *M* is given by

$$H = -\sum_{i=1}^{N} P_i Log_2 P_i \text{ (bits per symbol)} \qquad \textit{eq. 3}$$

This can be said to be the measure of expectation value of the novelty content of the symbol of a source. Therefore, and according to Eq.1 we may imply that the expectation value of the novelty content of a syntactic component is maximized when all symbols are equiprobable.

However, the most interesting implication is that this approach to the quantification of information accepts some prior knowledge on the part of the recipient, expressed in the respective probability distribution of the symbols from which the syntactic component is constituted. Indeed, the usage of structural units (identified as symbols) to construct a syntactic component from the signer, as well as their recognition from the relaying party, presupposes a certain prior knowledge in the form of a semantic agreement between them (Küppers, 1990). It is this semantic agreement that renders the consideration of the prior probabilities of the occurrence of each symbol possible. For this semantic agreement to work there should be two semantic levels. The specification of these two semantic levels is totally subjective. Hence, considering the symbols as the elementary unit of information, we can define the semantic level fixed by these symbols as *microstate*, while each other semantic level defined by the various combinations of these symbols, as *macrostate*.

Thus, information is defined in relation between two semantic levels, which makes the meaningful communication between the signer and the relying party possible.

As it is clearly stretched in (Floridi, 2004a), in Shannon’s theory information is only a selection of one particular microstate from the set of all possible microstates. The amount of information needed for this selection is the amount of the yes/no questions required to “guess” what the signer is communicating. It is the number of simple alternative choices needed to be made by the signer or the relying party in order to correspondingly create and describe the structure of the syntactic component. Therefore, the amount of information depends and varies accordingly to the level of the microstate to which the questions refer or on which the simple alternative choices are made. The respective questions are agreed and their answers (choices made by the signer) are decided with the appearance of the syntactic component. The probability of occurrence of the symbols of a microstate to which the question refers is the prior semantic knowledge of the relying party. As a result, the same sequence of symbols may contain a different amount of information.

In this sense, the informativeness of a syntactic component is the measure of the average amount of its structure. Consequently, the more unexpected the arrival of a syntactic component, the greater its informativeness, therefore, the greater the average capacity of its structural units, hence the more choices (information created by the signer) it can convey to the relying party.

4.1 Structural Informativeness as the Variety of the Syntactic Component

Based on the reasoning mentioned above, the source with the highest informativeness has the greatest structural capacity to inform. In a world where the purpose of communication would be solely to maximise the information within an agent, informativeness would be a sufficient and quite objective measure in order to decide regarding the suitability of the structural characteristics of a syntactic component. In the present case, where the objective is a fair digital signing, the ability of both the signer and the relying party to handle the structural capacity of the selected syntactic component should be secured. In this respect, informativeness, if it is to be used as a measure of its structural reliability, should be projected and used in the risky and demanding context of communicating a signed syntactic component. In this way, the structural reliability is constraint by the fact that the signer and the relying party should be involved in a digital signing on an equal basis.

In this perspective, the structural informativeness of a source can be seen as the measure of its variety, which represents the freedom of the source in making distinctions. The multiplicity of these distinctions is proportional to the uncertainty the source is able to create. The highest its uncertainty the greatest the variety of alternative selections one has to make in order to constraint the variety of the source and therefore to be informed. In the case of a signer and a relying party trying to communicate, the variety of the signed syntactic component acts as a measure of the perturbation on both their representational structures. Both cognitive systems should use the structural capacity of the signed syntactic component in order to be co-ordinated towards a certain state of affairs. As Ashby’s law of requisite variety suggests (Ashby, 1958; Heylighen, 2003) a system is able to compensate and control an external perturbation to the extent that it has sufficient internal variety to represent it. In other words, *the variety of the representational structure of both the signer and the relying party must be at least equal or greater than the variety of the syntactic component used in their communication*, for both of them to be able to fully exploit it towards their common goal.

Therefore, in the context of fair digital signing there is a limit in the structural capacity of the signed syntactic component to be used, which is upper-bounded by the lowest degree of variety among the representational structures of the involved parties. In the following sub-section the informativeness of various known (common) transformation protocols is computed and their usage in providing structurally reliable syntactic component to be signed is examined.

4.2 Computing the Structural Informativeness of Known (Document-based) Transformation Protocols

Focusing on the fact that applied transformation procedures transform the binary component into a formatted syntactic component, we proceed in computing the informativeness of various transformation (formatting) protocols. This provides us with a measure of the informativeness of the respective syntactic component, which is a measure of its structural capacity to inform. This component will be the tool based on which the signer and the relying party will try to co-ordinate regarding a certain state of affairs.

Specifically, working on the level of symbols we consider that a particular formatting protocol has an alphabet of *l formatting symbols*. For each chain of *n* formatting symbols of *l* different kinds, we have $M=l^n$ possible sequences of formatting symbols, thus, we have a number *M* of possible formatted digital documents consisting each time of *n* formatting symbols belonging to the respective formatting alphabet. The greater the *n*, the larger the respective document. Now, considering any one of the $M^{'}$ possible formatted documents, consisting of a number *N* of formatting symbols (so, $M^{'}=l^N$) of this particular formatting protocol, with {p_1, …, p_N}, where Σ(p[i]) = 1 as the probabilities of occurrence for each formatting symbol, the average structural information (informativeness) contained in this formatted document is given by the following equation:

$$H = -\sum_{i=1}^{N} P_i \log_2 P_i \text{ (bits per formatting symbol)} \qquad \textit{eq. 4}$$

In other words, we need a number of *H* binary (yes/no) decisions in order to decide upon each one of the *N* symbols of the formatting alphabet. Hence, *H* denotes the average capacity of the structural units used by the formatting protocol in the formatted digital document, which is the average number of choices (information created by the sender) each structural unit can convey to the receiver.

Therefore, working on the level of symbols we consider that a particular formatting protocol has an alphabet of formatting symbols (e.g. markup tags) plus an alphabet of lexical content symbols (e.g. the characters of Latin alphabet and the punctuation). For each type of document consisting of *N* formatting symbols (excluding the lexical content) we may compute the probabilities of occurrence for each symbol and the average structural information (informativeness) contained in this formatted document, based on the above equation *4*.

As a case study, we have chosen to compute the informativeness of six text-based document formatting protocols, being: plain-text, HTML, XML, RTF, PostScript and TEX, plus bitmap images. We have converted some documents (mainly with formatted lexical content, which is the usual case for digitally signed documents – e.g. the present paper) into all the above formats, assuring that their analogue representation looks (almost) the same, except, of course, of the plain-text document.

Pure binary and proprietary formats such as PDF and MS-Word are not included in the examined protocols since their syntax does not consist of distinct formatting symbols which can be distinguished from the content. Lacking of any better measure, we have counted the presence of distinct octets in the bit streams of the above binary formats. These symbols proved to be rather equiprobable (i.e. rather random) and therefore the value of informativeness is always computed at the highest possible value.

Document syntax	**Distinct Symbols (N)**	**Total Symbols (S)**	**Informativeness (H)**
TEX	256	853	4,581
RTF	400	6879	4,333
PostScript	1522	9958	4,191
HTML	124	1609	3,003
XML	47	1097	2,517
Bitmap	174	381214	1,567
Plain-text	3	832	0,412

TABLE I: THE INFORMATIVENESS OF DIFFERENT DOCUMENT FORMATS

For the plain-text document we counted as formatting symbols only the line feeds, the white spaces and the tabs. For the text-based documents with formatting capabilities, we counted the formatting symbols, being the distinct <> tags for HTML and XML, the strings between two backslashes (or a backslash and a space) for RTF, the strings within \ and space or '{' for TEX and the strings outside the brackets for PostScript. For the case of a bitmap image, we assumed that in an 8-bit color depth image the formatting symbol is a pixel, whose color is represented by an octet of bits. Thus, we counted each distinct octet in the bit stream as a symbol (i.e. maximum 256 different octets). The results of the case study are summarized in Table I. The values presented are the average of the examination of several different contents. *N* is the distinct symbols counted in each syntax, *S* is the total symbols and *H* is the computed informativeness.

The calculations show that TEX is the formatting protocol with the greatest informativeness. Thus, according to the previous analysis, the structural units used by the TEX format have the greatest average structural capacity to inform. However, each of the M' possible documents exhibiting a structure imposed by the TEX formatting protocol contains also the same amount of structural information. On the other hand, each one of the *K* possible documents consisting of an equal number of *N* formatting symbols, taking from another formatting alphabet (another formatting protocol) of lower informativeness, will contain a smaller amount of structural information. This means that with the occurrence of a formatting symbol of the TEX transformation protocol, the average number of the relying party's undecided binary alternatives that are being decided is greater than the respective number in case of the occurrence of a formatting symbol of the HTML transformation protocol, since $H_{\text{TEX}} > H_{\text{HTML}}$. The questions corresponding to these alternatives are agreed upon a priori, and they do not share any immediate relation with the use (at the semantic level) of the formatting symbol from the receiver. They are connected with the number of choices conveyed by a structural unit to a receiver, which are syntactically indicating, on the average, the variety of its possible use by this receiver. So, the structural capacity of a signed formatted document is proportional to the informativeness of the formatting protocol used for its transformation. In other words, its syntactic variety is lower-bounded by the specific transformation protocol.

4.3 Informativeness as an Indicative Measure for the Selection of the Most Structurally Reliable Syntactic Component due to Differences in the Semantic Variety

In the case of two agents trying to communicate through a document, there should not be any kind of constraint in the choice of the transformation protocol that should be used to format a given document. Since the essence of communication is the conveyance of as much information as possible, the use of the format with the greater informativeness would be the most appropriate. Things are not the same in the light of a signer and of a relying party, where there are legal expansions and penalties related to the creation and acceptance of a digitally signed document. Here, the structural reliability of the syntactic component and therefore its communication reliability, can be only subjectively measured and consequently selected.

Considering case *A1* (i.e. the structural characteristics of the syntactic component with respect to its ability to convey the signer's choices to the relying party are in a way compatible with the ability of both parties to intentionally interact with these characteristics) and aiming at performing fair digital signing, as it has already been argued, what should be secured, in order for the syntactic component to be structurally reliable, is that the variety of the formatted digital document should be in accordance with either party's semantic variety so that they would be able to purposefully interact with it. Consequently, acknowledging the values of the informativeness in Table I only as an indicative measure, it can be argued that the structural reliability of a syntactic component is a subjective measure, as it depends on the semantic variety of its user. Specifically, in the context of fair digital signing, the structural reliability of the syntactic component is maximized when its syntactic variety equals the semantic variety of both the signer and the relying party. Since this is hardly the case, for digital signing to be fair, and therefore, the syntactic component to be totally structurally reliable, its syntactic variety should be equal with the lowest semantic variety between the two parties.

The following example should clarify the issues discussed so far. We shall assume that a relying party interacts with a signed RTF-formatted digital document, which is in this case the macrostate consisting of concrete formatting symbols (i.e. \par, \tab, \li0, etc.) belonging to the microstate. In order for the relying party to be able to interact with the signed RTF-formatted digital document, she should first of all be able to recognise its structure as one which is somehow correlated with the structure of an RTF-formatted digital document, and thereby recognize its identity. At this point it should be postulated that the relying party (the recipient of the structural information) has the appropriate machinery for the incorporation of this kind of information. Hence, it is considered that the relying party combined with a reader (the computational system used to parse the formatted document in order to present it as a bitmap object in an analogue interface) of her own choice, are able to fully interact with the syntactic variety of the document. In particular, the relying party combined with the reader has some prior semantic knowledge expressed in the unexpectedness of the occurrence of each structural unit of the RTF-formatted digital document. The greater the information content conveyed with a particular structural unit, the more improbable its arrival. For example, the '\par' formatting symbol of an RTF-formatted digital document has an average structural capacity of a measure H_{RTF} to inform the relying party, which will be greater than the average structural capacity of the '<p>' formatting symbol of an HTML-formatted digital document, since $H_{HTML}<H_{RTF}$.

This does not mean that the one will be more or less clearly identified by the other, or that the one is better than the other. What we could safely argue is that on the average, the 'x' formatting symbol of an RTF-formatted digital document would have a greater variety than the 'y' formatting symbol of an HTML-formatted digital document. On the same basis, the macrostate representing a RTF-formatted digital document would on the average possess a greater number of possible microstates, which are represented by the respective formatting symbols, than a HTML-formatted digital document.

This implies that in a RTF-formatted digital document the relying party should anticipate an on the average greater variety of a sequence of formatting symbols. This implies a potentially greater variety of use of the RTF-formatted digital document by the relying party, which is absolutely acceptable when an ideal communication is the main objective. In this case, there are not and neither should be any constraints in the signer's and the relying party's choice or/and acceptance of a RTF-formatted digital document. In the case where signer's and relying party's co-ordination is the main objective, what has to be secured is that *they both have the knowledge and the capacity to handle the variety of the RTF-formatted digital document*, as this is directly related to its structural capacity.

4.4 Syntactic components and Human handlers

It has been argued that, in the context of fair digital signing, when the variety of the syntactic component equals the semantic variety of both the signer and the relying party, its structural reliability is maximised. In a real world environment this is hardly the case. Therefore, if the variety of a syntactic component (i.e. a RTF-formatted digital document) is higher than the semantic variety (prior semantic knowledge needed to be able to interact and fully exploit a RTF-formatted digital document) of at least one party (e.g. the relying party) involved in the digital signing, then the respective syntactic component is not deemed structurally reliable.

In this case, both parties should try to come to an agreement using a syntactic component of lower informativeness. Specifically, they should choose a syntactic component which the relying party thinks that she is able to fully handle. This does not mean that a syntactic component with the lowest possible informativeness (i.e. a plain-text formatted digital document) is always the most appropriate solution. In particular, a syntactic component (i.e. a plain-text document) that exhibits a syntactic variety lower than the semantic variety of both parties, cannot also be deemed, for this particular case, as structurally reliable. The signer and the relying party will be able to use it, but their co-ordination will not be the best possible. The semantic distance between them will not be reduced as much as possible. In this way, considering that they are both able to exploit a syntactic component with greater informativeness (i.e. an HTML-formatted digital document), they should decide to use it. Since it exhibits a greater variety, it is able to convey more choices of the signer to the relying party, hence it will support them to achieve a greater reduction of the semantic distance. In fact, for the preservation of the prerequisite of supporting a fair digital signing, they should choose the syntactic component with the highest informativeness that they will both be able to handle.

However, in the extreme case where both the signer and the relying party have limited prior knowledge regarding any formatting protocol, the syntactic component with the lowest informativeness, (i.e. a plain-text formatted digital document, which exhibits the lowest syntactic complexity) should be preferred.

The abovementioned presumptions can be summarized in the following table:

Combination of:		**Results in:**
Syntactic component	**Human handler**	
High syntactic variety	High and compatible semantic variety	Reliable digitally signed communication. Best mitigation of semantic distance
High syntactic variety	Low or incompatible semantic variety	Unreliable digitally signed communication.

Low syntactic variety	High semantic variety (much higher than the syntactic component)	Poor communication (unused communication capabilities)
Low syntactic variety	Any user with at least the same low semantic variety	Reliable simple communication on the syntactic level but not on the semantics.

TABLE II: THE COMBINATION OF DIFFERENT TYPES OF SYNTACTIC COMPONENTS WITH DIFFERENT TYPES OF HUMAN HANDLERS

It is now clear how the proposed framework helps addressing the attacks mentioned earlier, where an adversary could modify the lower-level representations without invalidating the digital signature. Ideally, the relying party should read the raw binary data and be able to manually make the necessary transformations in order to perceive the communicated message. Only a few people in the real world would do that, but it is not unfeasible that this procedure should be done for some critical parts or some samples of the signed message. In case the relying party is able to successfully transform the raw data into the expected final representation using exclusively his/her own means, the signature could be trusted.

Using a high-informativeness protocol for transferring a message would enable the communication of more semantic information compared to a lower informativeness protocol. At the same time, an attacker could benefit from the high informativeness in order to alter the perceived representation of the data, for example by hiding information, by referring to external unsigned sources or by manipulating the parser of the document. However, in case the relying party is aware of the protocol(s) used and able to handle it, the attack is very difficult. For example, a relying party who receives an HTML document should be able to handle at least the character encoding protocol (e.g. ASCII) and the formatting protocol (HTML) while being compatible with the document (i.e. language used). If the relying party is able to safely parse the raw data, the signature may be trusted, otherwise the signature must be rejected.

5. Qualitative evaluation of the Structural Integrity of the Syntactic Component

In the previous sections it has been argued that if a zero distance at the syntactic and presentation level is postulated, the measure of informativeness can be used as a measure for the selection of a syntactic component as structurally reliable. Moreover, it has been argued that is not an absolutely objective measure. It is an indicative measure which sets the limits of the communication reliability of the syntactic component in a specific situation. It supports its selection as the most structurally reliable in relation to the semantic variety of the involved parties regarding the respective syntactic component.

In case of an introduction of a distance in the syntactic and presentation level the binary component could be differently transformed (both in the part of the signer and the relying party) disregarding the rules of the respective formatting protocol. In this case, the structural integrity of the resulting formatted and signed syntactic component would be compromised. Now, for the syntactic component to be structurally reliable, its structure should support the prerequisites discussed in the previous sections with respect to its users, but it should also have the ability to better compensate the possible loss of its integrity. It is noted that the integrity of the binary data (binary component) is secured by the application of a digital signature (see Figure 2) and the lexical content is assumed to be the best possible. Here, the quantitative measure of informativeness alone cannot provide us with an equivalent measure for the capability of a syntactic component to better compensate its possible structural damage.

However, focusing on the transformation procedures applied on the binary component, we may identify several qualitative parameters of various transformation protocols that affect the structural reliability of the relevant syntactic component. Indeed, some of these parameters increase or reduce the ability of the syntactic component to restore the damage on its structure. Some of these parameters are related to the informativeness of the respective documents, while some others are not.

The parameters taken into consideration are related to the notions of semantic distance and of structural reliability and they are divided into two basic categories:

<u>Integrity on the syntactic level:</u>

- *Existence of meta-data*: The intrinsic capability of the protocol to include customized meta-data within its signed part, is a positive characteristic. For example the inclusion of the type of the document, the protocol and the version used and other descriptive information increase the objectivity of the transformations and thus the structural reliability. Additionally, the existence of meta-data adds a '*predefined logic'* between the communicating parties that will reduce the semantic distance of the exchanged messages. Meta-data are common in markup languages, such as HTML and especially in XML.

- *Embedded transformation protocols*: A document capable to include the parser or the transformation protocol within its body before it is signed, reduces ambiguity and increases the lexical content reliability. Postscript and PDF for example are supporting the embedding of character encodings.

- *Existence of canonicalization rules*: Canonicalization acts complementary to a transformation protocol, imposes the construction of well-formed documents and contributes to the elimination of ambiguities in the transformation of digitally signed documents. It enhances the communication reliability between the two communicating parties.

- *External references*: The usage of (not signed or standardized) external references such as style-sheets or character encoding protocols increase document ambiguity and may result to unexpected results. This parameter is related with the syntactic distance that can be added due to ambiguities in the application of syntactic rules, alphabets and encodings on the binary component. It is obvious that in such a case the structural integrity of the respective formatted document will be damaged. External references, such as style-sheets, character encodings and other data sources are common in markup languages, but they can be completely avoided in Postscript documents.

- *Dynamic formatting*: Documents that include dynamic format produced by non-deterministic code or scripts that display arbitrary results within the document also increase ambiguity and reduce the structural reliability.

The lack of Integrity on the syntactical level is exhibited in our previous preliminary work (Lekkas, Arnellos, Spyrou & Darzentas, 2005) where a real example of documents with external references and lack of canonicalization may lead to false positives and false negatives during the validation of a digital signature.

<u>Readability on the syntactic level:</u>

- *Openness and Standardization*: A public, widely available and standardized protocol gains advantage (in terms of objectivity) against unknown proprietary protocols. In case a formatting protocol is widely available and standardized the users are able to track down and identify its symbols. This adds to their capacity to distinguish the formatting symbols and to make the transformation without using a computational system. It increases the readability of the formatting protocol by enhancing the structural informativeness of the used protocol

- *High Readability*: In the context of the present analysis we consider a protocol having high readability when its formatting symbols can be easily identified and distinguished from a human and/or when a human can perform the formatting transformation process and follow the results without using a computational system. On the contrary, a protocol has a low readability when it is very difficult or almost impossible for a human to identify and distinguish its formatting symbols and/or it is difficult or practically impossible for a human to reproduce the result. According to this definition, a highly-readable (human-transformable) document exhibits much more objectivity, since it can be more easily trusted by humans (signer and relying parties). The problem of human-transformability of a protocol can be almost directly related to its informativeness. As it is argued above, informativeness is considered as a measure of the equiprobability of the occurrence of the formatting symbols of a formatting protocol. Additionally, it is affected by the total number of symbols a certain formatting protocol supports. Therefore, in a highly informative formatting protocol, even if each symbol is highly distinguishable, on the average, the variety of combinations between different formatting symbols will be great. This will impose a further difficulty in case a human try on her own to perform the transformation process and produce the respective bitmap object. It can be argued that formatted digital documents exhibiting low informativeness would on the average have a higher readability than documents exhibiting a lower one. Accordingly, we may argue that markup languages are more readable than TEX, RTF and PS formats. The problem of the identification of each symbol is related to the degree of publicity and standardization as described below.

5.1 Relation between the qualitative parameters and the metric of Informativeness

The inclusion of customised meta-data regarding the transformation protocol, as well as the inclusion of information regarding the operations of the transformation protocol into the signed part of the syntactic component, increases the *redundancy* of the respective formatted syntactic component. In the safe situation of the *A1* case, redundancy is what can be abstracted from the syntactic component without any reduction in its communication reliability. But in the case where a possible loss of structural information is possible, redundancy can be used for the recovery of this information. Hence, it operates as a capacity for error correction in the structure of the syntactic component. As such, redundancy can be modelled as the insertion of new formatting symbols (playing the role of formatting-related meta-data, or data related to the execution of the transformation procedures) in the syntactic component, while keeping the number of the other formatting symbols fixed.

The following analysis demonstrates the relation between the increment of redundancy (the insertion of new symbols) and the behaviour of the informativeness in a transformation protocol. We investigate the insertion of a new formatting symbol into an existing document and what is the effect of this insertion in the metric of informativeness.

We consider that an initial document has *S* total symbols, *N* distinct symbols used, *H* is its initially computed informativeness, K_i is the times of appearance of symbol i and P_i is the probability of appearance of symbol i.

A new *(N+1)th* non-existent symbol is now inserted into the document and *M* is the times of appearance of this new (unique) symbol. P'_i is the new probability of appearance of symbol i after the insertion of M total symbols and *H'* is the new value of Informativeness.

Initially:

$$H = -\sum_{i=1}^{N} P_i * Log_2 P_i$$

$$P_i = \frac{K_i}{S}$$

The new probability of appearance of a symbol i after the insertion of the *M* symbols is computed as:

$$P_i' = \frac{K_i}{S+M} = \frac{K_i * S}{(S+M) * S} = P_i * \frac{S}{S+M}$$

We easily compute the new Informativeness *H’* as follows:

$$H' = -\sum_{i=1}^{N+1} P_i^{'} * Log_2 P_i^{'} \; = \; -\sum_{i=1}^{N} P_i^{'} * Log_2 P_i^{'} \; + \; P_{N+1}^{'} * Log_2 P_{N+1}^{'} \; =$$

$$= -\sum_{i=1}^{N} P_i \; * \frac{S}{S+M} * Log_2 (P_i \; * \frac{S}{S+M}) \; + \; \frac{M}{S+M} * Log_2 \frac{M}{S+M} =$$

$$= -\sum_{i=1}^{N} P_i \; * \frac{S}{S+M} * (Log_2 P_i \; + Log_2 \frac{S}{S+M}) \; + \; \frac{M}{S+M} * Log_2 \frac{M}{S+M} =$$

$$= -\frac{S}{S+M} * \sum_{i=1}^{N} P_i \; * Log_2 P_i \; - \; \frac{S}{S+M} * Log_2 \frac{S}{S+M} * \sum_{i=1}^{N} P_i \; + \; \frac{M}{S+M} * Log_2 \frac{M}{S+M}$$

By substituting $1 = \sum_{i=1}^{N} P_i$ and $H = -\sum_{i=1}^{N} P_i * Log_2 P_i$ we conclude that:

$$H' = H * \frac{S}{S+M} \; - \; \frac{S}{S+M} * Log_2 \frac{S}{S+M} \; - \; \frac{M}{S+M} * Log_2 \frac{M}{S+M}$$

And finally:

$$H' = \frac{H * S \; - \; S * Log_2 S \; - \; M * Log_2 M \; + \; (S+M) * Log_2 (S+M)}{S+M}$$

According to the above formula, the insertion of a new symbol is always increasing the value of informativeness of the document, while the repetition of the new symbol M times, will decrease the informativeness for a large value of M.

The threshold that determines the behavior of the informativeness is the value T below, which depends on the value M:

$$T = \frac{S * Log_2 S \; - \; M * Log_2 M \; + \; (S+M) * Log_2 (S+M)}{M}$$

If T > H, then the informativeness will increase after the insertion of the symbols, otherwise it will decrease.

The curve of the resulting new informativeness is shown in Figure 3 for a given S and H of a document (say S=1000, H=5) and illustrates the above conclusions:

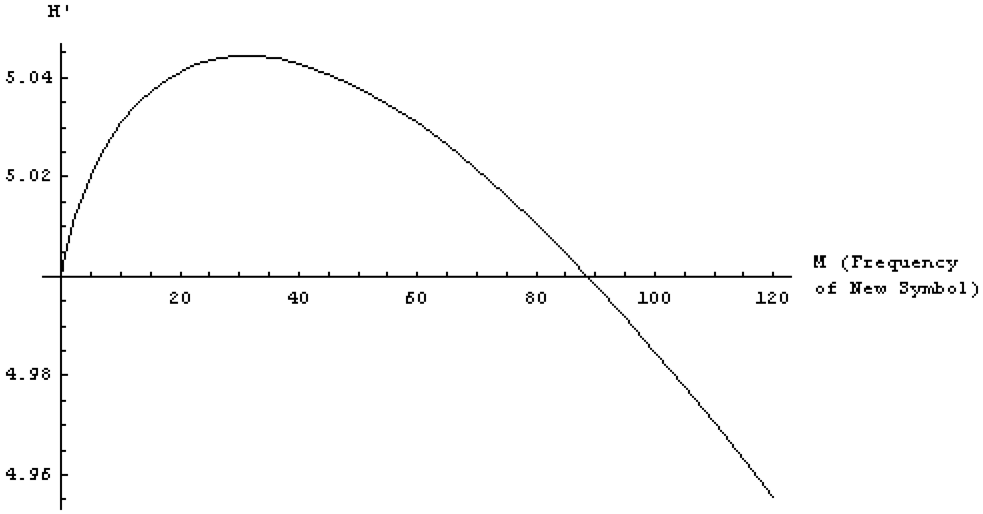

Figure 4: The behavior of informativeness after the usage of a new symbol

As a conclusion, it is shown that some of the characteristics described in section 5 that increase the redundancy of a syntactic component (e.g. the existence of meta-data and the embedding of transformation protocols) are directly connected to the value of informativeness. Since they increase the number of symbols used, they generally increase the informativeness of the document. However, this holds only until a threshold in the appearance frequency of the new symbols is reached.

6. Conclusions

We introduced a framework describing the intentional signing action and the way meaning is created when a signer or a relying party interacts with the digital document. Based on this framework it has been argued that the semantic distance between the interacting parties is inevitable and it should be presupposed in any application of a digital signature. Hence, under the perspective of fair digital signing the main objective is to reduce the semantic distance, providing the involved parties with favourable conditions for mutual understanding. Based on the described framework, it has been argued that the semantic distance produced by the interaction of the involved parties with the formatted digital document depends on its structural and lexical reliability. Consequently, by increasing the structural reliability of the syntactic component (which is approached as a distinct level in the communication process) we manage to mitigate the semantic distance.

The capacity of a syntactic component to inform is indicated by the metric of the informativeness of the formatting symbols used in the syntax in which the syntactic component is expressed. In general, in a fair digital signing context, the choice of a formatting protocol that renders the resulting syntactic component the most structurally reliable, primarily depends on the semantic variety of the users in respect to this protocol. Particularly, it is argued that, in case there is no noise introduced in the syntactic and presentation level, the most structurally reliable syntactic component will be the one which will use the formatting protocol with the highest informativeness, as long as it is equal or lower than the semantic (representational) variety of the involved parties. In the extreme cases where both parties have no prior knowledge regarding any formatting protocol, the syntactic component using the one with the lower informativeness is deemed as the most reliable and secure to be used.

The informativeness of several well-known formatting protocols has been calculated and can be used as an indication for the selection of the syntactic component supporting a fair digital signing process. In the case where noise is introduced in the syntactic and presentation level, it has been argued that informativeness alone cannot provide us with a measure in order to choose the syntactic component that will better compensate its structural damage. Some other qualitative parameters of the formatting protocols are identified, which increase or reduce the ability of the syntactic component to mitigate or restore the possible damage. Some of these parameters proved to be directly related to the value of informativeness, since they indicate an increment of redundant formatting symbols. The value of the informativeness in respect to the increment of symbols is initially augmentative, and therefore the structural reliability of a digitally signed formatted document is further strengthened.

Several countries have implemented laws related to digital signatures enhancing the EU legislation. Some of these laws already recognize the requirement for "fair digital signing" by enforcing mandatory document formats, parsers that support the notion of "what you see is what you sign" and disallowing dynamic content. All the above legal requirements focus on reducing the syntactic variety of the documents and thus the proposed framework proves that they are to the right direction.

References

Adams C., Cain P., Pinkas D., Zuccherato R., "Internet X.509 Public Key Infrastructure Time-Stamp Protocol", IETF Request For Comments 3161, available at http://www.ietf.org/rfc/rfc3161.txt , 2001.

Alsaid, A., & Mitchell, C. (2005). Dynamic content attacks on digital signatures. *Information Management & Computer Security* , pp. Vol. 13 Iss: 4, pp.328 - 336.

Arnellos, A. , Lekkas, D., Spyrou, T., Darzentas, D., "A Framework for the Analysis of the Reliability of Digital Signatures for Secure E-commerce", The electronic Journal for e-commerce Tools & Applications (eJETA), Vol.1, No.4 (2005)

Ashby, W. R., "Requisite variety and its implications for the control of complex systems", Cybernetica, 1, 1958, p.83-99

Bar-Hillel Y., Carnap, R. "An Outline of a Theory of Semantic Information", rep. in Bar-Hillel, 1964, p.221–274.

Christensen, W.D., Hooker C.A., "Representation and the Meaning of Life". In: H. Clapin, P. Slezak and P. Staines (eds), Representation in Mind: New Approaches to Mental Representation, Westport: Praeger, 2004

Cooper D., Santesson S., Farrell S., Boeyen S., Housley R., Polk W., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", Request for Comments 5280, May 2008

European Union Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 1999

Floridi L., "Information", In: The Blackwell Guide to the Philosophy of Computing and Information, edited by Luciano Floridi, 2004a, p.40-61.

Floridi L., "Outline of a Theory of Strongly Semantic Information", Minds and Machines 14, p.197–221, 2004b, Kluwer Academic Publishers.

Girault M., "Self-certified public keys", In: Advances in Cryptology: Eurocrypt'91, LNCS 547, Springer-Verlag, 1991, p.490-497.

Greenberg M. and Harman G., “Conceptual Role Semantics” in *The Oxford Handbook of Philosophy of Language*, edited by Ernest Lepore and Barry Smith, 2006.

Heidegger, M., “Being and Time”, New York: Harper and Row, 1962.

Heylighen, F., “The Science of Self-organization and Adaptivity”, In: Knowledge Management, Organizational Intelligence and Learning, and Complexity, In: The Encyclopedia of Life Support Systems, EOLSS Publishers Co. Ltd. 2003.

Josang A., Povey D., Ho A., “What You See is Not Always What You Sign”, In: proceedings of the Australian UNIX User Group, AUUG’02, Melbourne, 2002

Kohnfelder L., Towards a practical public-key crypto-system, Thesis, MIT, 1978

Küppers, Bernd-Olaf, Information and the Origin of Life. Cambridge, MA: MIT Press, 1990.

Lekkas D., Arnellos A., Spyrou T., Darzentas J., “Pervasive Digital Signatures: Syntactic robustness and simplicity of signed documents”, In: Proceedings of SecPerU'05, Security, Privacy and Trust in Pervasive and Ubiquitous Computing, Santorini, Greece, IEEE, 2005, p.21-28

Lekkas D., Gritzalis D., “Cumulative notarization for long-term preservation of digital signatures”, Computers & Security, 23, 5, 2004, p.413-424.

Maurer U., “Intrinsic limitations of digital signatures and how to cope with them”, in Proceedings of the 6th Information Security Conference (ISC'03), LNCS-2851, 2003, p.180-192.

McIntosh M., Austel P. “XML signature element wrapping attacks and countermeasures”. In Proceedings of the 2005 workshop on Secure web services, ACM.

Merleau-Ponty, M., “Phenomenology of Perception”, Trans. Colin Smith. London: Routledge and Kegan Paul, 1962.

Mingers, J., “The Nature of Information and its Relationship to Meaning”, in R. L. Winder et al., Philosophical Aspects of Information Systems (London: Taylor and Francis) 1997, p.73-84.

Rapaport W.J., “Holism, Conceptual-Role Semantics, and Syntactic Semantics”, Minds and Machines 12(1), 2002, p.3-59.

Rapaport W.J., “Understanding Understanding: Syntactic Semantics and Computational Cognition”, in James E. Tomberlin (ed.), AI, Connectionism, and Philosophical Psychology, Philosophical Perspectives Vol. 9 (Atascadero, CA: Ridgeview): 1995, p.49-88.

Rivest R.L., Shamir A., Adleman L., “A method for obtaining digital signatures and public-key cryptosystems”, Communications of the ACM, 21,2, 1978, p.120-126.

Schneier, B. (2000). *Why Digital Signatures Are Not Signatures.* Crypto-Gram,Counterpane Internet Security, Inc.

Searle, J. R., “Is the brain a digital computer?,” Proceedings and Addresses of the American Philosophical Association., 64, 1990, p.21-37

Shannon C. E., Weaver, W., “The Mathematical Theory of Communication”, Urbana and Chicago, IL: University of Illinois Press, 1998.

Zeevat H., “The Asymmetry of Optimality Theoretic Syntax and Semantics”, Journal of Semantics, 17, 2002, p.243-262.