

The Possible Laws on Digital/Electronic Signature: On the Proposed UNCITRAL Model

Pedro A. D. REZENDE
Department of Computer Science
University of Brasilia; Brasilia DF Brazil
Tel. (55)(61) 3072702; email: rezende@cic.unb.br

ABSTRACT

What is the connection between the UNCITRAL model for electronic commerce laws and the U.S. 2000 presidential election imbroglio? How does this connection, if recognized, resonates certain milestones of our civilization's heritage, legacies from the Phoenicians and from the Roman empire? There is something basic about human communication and reasoning which weaves through these themes, in the way our languages work: trust. And the moment seems ripe for reflecting upon the weaving of trust thus produced. This article offers some personal views on an astonishingly neglected dimension of the virtualization of our social processes, set in motion by the digital revolution, in which the underlying texture of trust ceases to be treated as a transparent veil.

Keywords

Digital Signature, Electronic Signature, Authentication, Law, Model Law, Cryptography.

INTRODUCTION

Classification of Laws

A recent report by the U.S. Library of Congress [1] describes concepts and approaches of 76 laws on electronic signature already enacted or proposed within the US, and attempts to classify them in three models. These three models are described by this report according to chronological prominence, where criticism of the earliest two are echoed. The first model is called "prescriptive", for regulating directly on the use of Public Key Infrastructures. The second is called "criteria based", for establishing functional thresholds of reliability and trustworthiness to which a digital authentication mechanism must adhere, in order to be accepted as substitute for handwritten signatures in electronic documents. The third model, named "signature enabling", is not criticized and is given a vague description, through the assertion that it "*recognizes electronic signatures and documents in a manner parallel to traditional signatures*". To these claims the report mixes another, about technological neutrality, as alleged advantages for third model laws, construed as justification for it. Since the third model grants to market forces the power to decide what constitutes an electronic signature, it can more appropriately be called "grant" model, as done here.

Legislatures over the world are under pressure to enact laws intended to propel electronic commerce. In a recent conference, two proposals for legislation regulating the use of electronic signatures currently under consideration by the Brazilian Congress were discussed. With honorable exceptions, the invited speakers were unanimous in praises to a proposal drafted according to the UNCITRAL model, and in criticisms directed

at the proposal drafted by the Brazilian Association of Lawyers, the OAB. The debate that followed in cyberspace has induced the reflections presented by this article.

In our view, the most serious risks with the prescriptive model are not in obsolescence, as often pointed, but in the total and complete responsibility of the owner of a private key, for its safekeeping. This is because the handling of keys has to be intermediated by software whose reliability and trustworthiness the owner of the key does not know how to fathom. The digital signature law of the state of Utah -- the first ever enacted --, those of Italy, Spain and France, and Brazil's OAB draft, follow the prescriptive model at some regulatory level. To such risks in the first model, the second model adds the danger of covering digital authentication mechanisms with an aura of trust, for there is at present no known safe method for measuring trust in these mechanisms [2]. And none in sight. The second model was chosen by the state of California in drafting and approving its digital signature law. Risks from the former two models are compounded in the third by the potential abuse of social agents whose economic power allows them to impose mechanisms they choose. The logic for their choice unbalances the risks and responsibilities endowed by intent or consent recorded through the use of such mechanisms, whereas the balance of such risks should be the objective of such laws. The grant model was chosen by the state of Massachusetts, and is the basis for the recently promulgated U.S. federal law known as e-Sign [1].

Comparing Models

This article attempts to show the magnitude and depth of risks inherent to legislation based on the grant model, as well as the merits of the prescriptive model, which have been conspicuously absent from academic discussions regarding this new law making process. We shall avoid being side-tracked by the subject's complexity, suspending judgement about a simplistic approach to this legislative process being necessarily better. We are sailing uncharted juridical waters, in which the law is to rule over diaphanous things, whereas machines are to generate and manipulate symbols purported to represent human intentions. The mere mention of this purporting in law is not enough for its efficacy, as will be argued. To start this argument we observe, for comparison, what lurked behind the dispute over Florida's 2000 presidential election results, regarding legal inefficacy. A juridical vacuum set up by laws which only mention such purporting, where the circumstances and levels at which humans themselves are required to play active roles in the interpretation of machine-conducted meaning is not clearly addressed by the statutes. As a consequence, different levels and circumstances were deemed right by contenders as they saw fit, while scarce and tenuous jurisprudence available for arbitration muddled the difference between interpreting and rewriting applicable law.

TECHNOLOGICAL NEUTRALITY AND SEMIOTIC CLARITY

Separating Concept from Technique

The main argument in favor of the grant model, surmised in that report [1], sustains that a law regulating the use of digital or electronic signatures shall not delve into technology. The law would risk rapid obsolescence in so doing, and shall therefore restrain itself to conceptual framing. The regulatory aspect of how such framed concepts are to be achieved and deployed through available technology, or whether it is being achieved by deployed mechanisms, is to be left for competent institutions to address, such as canvassing commissions in the comparing example, or the free market, as posited by defenders of the e-Sign law [3]. This argument follows the Anglo-Saxon juridical tradition and may look sound at first glance, but presupposes underlying, often overlooked, beliefs. Those on the legislator's ability, competence and will to separate, for this kind of law, concept from technique.

So what is *system*? What is *concept*? What makes a definition *technical*? What is *law*, in cyberspace? It should be regarded as common sense that a law shall describe its object whenever such object is not settled in the culture of the language in which the law is written in. For other cases, dictionaries and jurisprudence may furnish them. Signature on bits is something that is not settled in any culture, for we have vendors, lobbyists and cryptographers waving different explanations about what it may be, differing markedly in functionality and potential legal implications. No human language has settled to date what this thing is, and nothing being said about it is going to change the fact that we are dealing today with a deeply ambiguous, almost mythical concept. If the law fails to do it, implementors, regulators and contestants will define what this object of laws is, and the laws' effect may become the opposite of what the argument for the grant model tries to achieve, as with those electoral statutes: efficacy.

There is a delicate line drawn by ambiguity, in the process of making laws, separating efficacy from danger. In the Florida vote imbroglio, the statutes were technologically neutral but semiotically muddled. For those circumstances in which the measuring by machines of voter's "*clear intent*" accrues insufficient precision, the statutes lacked enough provisions for routing arbitration. Digital signature laws resemble modern electoral statutes in so far as both need to address machinable representations of human intent. There are compelling reasons for technological neutrality in these laws, but even more compelling reasons for semiotic precision. As explained by Lawrence Lessig, a Harvard professor of constitutional law insightfully observing the judicial process meet the virtual, in cyberspace the law is the software [4]. The mass deployment of improperly conceived ethereal signature systems under broad and vague jurisdiction may force citizens to accept, as records of their own will and consent in electronic documents, marks whose issuance is not necessarily linked to their perceived interaction with computers. Therefore the importance of reliable public knowledge and auditability of these systems' inner logic, to warrant their public acceptance. Are we to be given only the hope that these guarantees will come voluntarily?

A Crossroads

The need for laws instituting digital or electronic signatures, brought about by e-commerce and its globalized environment, takes our civilization to a crossroads. Societies have to choose, as we intend to show how, between two paths. In one of these paths the compass points towards the preservation of common

law jurisprudence, through the regulatory process for emerging new forms of commerce. Through it, the functionality of new forms of signature has to approximate that of the handwritten signature, for the balance of risks and accountability reached through millennia of social practice debugging is sought to be maintained. This balance is embodied in various codes of rights. Of those, one regarding signatures is the right of an alleged contracting party to repudiate forgeries -- the repudiation right. And its counterpart is the right of a party to seek arbitration for repudiations against him -- the non-repudiation right. We may call this possible path the path of prudence.

The other possible path is to be taken in the name of progress. Its ideology claims that we can, and shall, do away with tradition for the sake of economic efficiency. The compass there points to a mere adjectivation of the lexical definition of signature, aiming at endowing it with an extra, virtual meaning. In this path a long-standing tradition, in which the signer controls the difficulty of forgeries against him (by creating himself the mark which will socially identify him), is to be neglected by new signature laws [5]. We see this path as issuing a blank check to capital, giving it unprecedented powers. On this path's cybercultures, people will ignore the source of trust demanded of them in acknowledging their own commitments, as recorded by bits, in a redemption of slavery only this time in a fuzzy and ethereal form. This path can be called the path of greed, and we can note that political powers in contemporary democracies, left to themselves, are inclined to choose it.

We claim that the choice of model for a digital signature law reflects the choice a society makes on this crossroads. To sustain this claim, we will examine the structure and context of the argument for technological neutrality, as employed both to defend the grant model and to criticize the prescriptive model. The context in which this argument has been so employed has as background the possible classifications of methods for digital authentication. This context lumps together some of these methods under a label, of one among the so called "electronic signature technologies". Such methods are cryptographic processes based on asymmetric cipher algorithms, taken by the prescriptive model as basis for its conceptual framing.

Common (mis)Use of the Neutrality Argument

To analyze the structure of this argument we begin by looking at its use of language. Not all virtual stuff is technology, and an impression to the contrary seems to come from a deliberate noise. Asymmetric cryptography is a semiotic concept, and to mistake this concept as a technology is fallacious. We believe that legislators, lobbyists and counselors who engage the technological neutrality argument for the purpose of promoting the grant model against the prescriptive model are being excessively generous in their self evaluation of competence to distinguish technology from semiotics. And we also believe that there are grave social risks in this generosity, which portrays the prescriptive model as an attempt to lock one specific technology as the legal definition of digital signature. What the prescriptive model, in fact, locks to such definition, is the functionality any digital authentication method must have, to be able to translate a property held by handwritten signatures onto the digital realm. This property is the control that a signer has the discretion to exercise, over the difficulty a verifier will face to be able to forge his signature. Furthermore, this locking shall not be construed as a political or technical cast, for it is, in fact, a logical deduction of causal nature, within the scope of a mathematical theory of information.

THE NATURE OF ASYMMETRIC CRYPTOGRAPHY

What is Asymmetric Cryptography?

The term "asymmetric cryptography" literally means "writing capable of non-symmetric concealment" [6]. The three substantives in this Greek etymology refer respectively to language, geometry and cognition, perennials that are independent of any technique or any law ever created by men, predating and outliving any of all civilization's juridical and technological systems. The concept of asymmetric cryptography is akin to others we already know from semiotics, such as alphabetic writing and ideogrammatic writing, positional numeric writing (yielding the binary and decimal systems) and non-positional numeric writing (yielding the Roman system).

The thought that a digital signature law will lock in an obsolescence-bound technology by being prescriptive, reflects a profound confusion arisen from taking to be a technology what is actually a semiotic concept. This concept is deduced from what must be required of the virtual world for securing today's necessities of the live world. These necessities would change only if the live world would too, to a point where men become so honest that one would no longer worry about the possibilities of one's personal mark of intent or consent being forged in electronic contracts, due to protocol flaws, or negligence or bad faith by those who need to verify the legitimacy of these marks. This may not be the kind of obsolescence worrying those who think of asymmetric cryptography as ephemeral technology.

The process leading from necessity to semiotic concept is not a novelty. The alphabetical writing arose from the necessity to facilitate the learning of written language, reached through the binding of its systems to the phonetics of spoken languages. Positional numeric writing was derived from the necessity to facilitate learning and automation in mathematics, in whose systems the methods for doing arithmetic would be effective and fixed, for any order of magnitude of operands. Asymmetrically concealable writing is just the latest and perhaps the most revolutionary semiotic concept that human intellect has been able to grasp and deploy, out of necessity for a certain kind of authentication. Namely, the kind of authentication able to offer, in a virtual and hostile world, functionality for some level of self control over forgeries and spurious repudiation.

Comparing Different Types of Risk

The neutrality argument, employed to target the prescriptive model, qualifies it as naive and risky, on the assumption that what the model prescribes is technology bounded for obsolescence. This assumption, without further elements to justify the classification of asymmetric cryptography as technology, places such classification above that of the functionality offered by the target. This logical setting for the neutrality argument is less grounded than the recognition of its target as a new semiotic concept, besides naive and risky itself, since it implies a belief that future technologies will dissolve our need for cautionary practices against unwanted byproducts of human selfishness and greed. To remind ourselves, such byproducts include forgeries and dishonest repudiations. On the other hand, to sustain that asymmetric cryptography is a semiotic concept, and not technology, is also naive and risky, but for quite different reasons than those suggested by the use of the neutrality argument to target the prescriptive model.

The current use of the word "*technology*" is amusing, but also dangerous. It is quite often employed to conceal ignorance about the insides of a given object of speech, as well as to offer an agreement for mutual acceptance of such concealment. And not

less often, as magic wand for credulity spells. And frequently, as both. The belief that semiotics and technology are the same thing, that "*concept*" and "*system*" have identical meanings, is naive and dangerous for reasons we shall give. And claiming the opposite is naive and dangerous too, since few would grasp its importance and powerful interests would be annoyed. We shall also ponder the reasons for this annoyance, while for now we note that the main difference between dangers and naivetés in these opposing postures lay in the quality of conscience supporting the acceptance of implied risks.

Semiotics is not technology. Concept is not system. Concept is a linguistic phenomenon, while system or technology -- as employed in the neutrality argument to target the prescriptive model -- is a material phenomenon [7]. Asymmetric cryptography is a semiotic concept, not technology. Technology is RSA, El Gamal, ECC or DSA, mathematical constructs that have been discovered to substantiate such concept, expressed in the form of protocols and cipher algorithms. Unlike the concept of digital or electronic signature, the concept "*semiotics*" is already sedimented in our cultures and we can rely on the dictionary to understand its meaning. We claim that asymmetric cryptography is the only concept that prudently deserves to be taken as framework for a legal definition of digital or electronic signature, specially for use in contracts, because it is a concept derived from necessities that handwritten signatures have been effecting for contracts in paper, since the inception of this type of instrument. To support this claim, we offer to explain this derivation, after a brief overview of comparative history, to clarify its role.

SELF CONTROLLED AUTHENTICATION

A Historical Perspective

The use of new signs to represent sounds is at the core of alphabetical writing. The use of a new numeral to represent nothingness -- the zero -- is at the core of positional numeric writing. The concept of zero is the only concept capable of yielding automation technologies for arithmetic, such as the calculator and the digital computer. Any such technology is substantiated by a positional system for representing numbers, such as the computer's binary, the Arabic's decimal and the Mayan's vigesimal (we have 20 fingers), the ones used to date. With them, automation of operations can be achieved, with the use of tables. In likeness, the use of a non shared secret in a key of a pair -- the private key, which forms a pair with its inverse, the public key -- is at the core of asymmetric cryptography. The concept of private/public keys is the only concept capable of yielding automation technologies for issuance and verification of unique personal authentication marks on digital documents. Any such technology is substantiated by an asymmetrically concealable writing system, such as the RSA, ECC and DSA, the effective ones discovered to date. With them, identification marks in digital documents which can truly be called unique and personal are achieved, with the use of non-shared secrets.

A numerical representation system will be positional or not, depending on how it employs the numeral zero. This classification holds for any system, yet discovered or not, intended to represent numbers. A digital authentication system will be cryptographic or not, depending on whether or not it employs secrecy. And in case it does it will be asymmetrical or not, depending on how it employs secrecy. Again, this classification holds for any digital authentication system, already invented or not, and over this fact there is nothing to discuss

among those who understand the matter. The tricky problem with signatures on bits hovers around attempts to merely adapt the lexical definition of the concept, towards its virtual usage. If we look at how this lexical definition stood before the advent of modern computers, we find the following.

From 1955 Webster's: "Signature",

"1. a person's name written by himself, or a representation of this by a mark, stamp, etc.", or

"2. the act of signing one's name", to which the verb means

Verb, transitive or intransitive: "To Sign"

"1. to write one's signature, as in attesting or confirming something" (intransitive)

"2. to write one's name on, as in acknowledging authorship, authorizing action, etc.", (transitive) [8]

To make sense of an adjectivation specifying on what thing a certain type of signature is to be written, in which this thing is a sequence of bits, and therefore a non-physical thing, one has to know how a personal and unique mark can be made virtual. This knowledge is necessary, sooner or later at the judicial arena, for selecting, among digital authentication methods, those that can be competent and effective substitutes for handwritten signing in legal documents, if traditional common law jurisprudence is to be upheld. Non-repudiation rights for example, can only be sustained if this knowledge is asserted for the authentication method employed. We posit that a digital/electronic signature law cannot omit or delegate this knowledge, while still seeking its current publicized purpose and intended efficacy, since doing so, either for the sake of simplicity or in disregard of such knowledge, will imply the forceful abandonment of traditional common law jurisprudence.

Knowing the Signature's Functionality

This article intends to reassure the fact that this knowledge has been produced by a mathematical theory of information, being at reach of lawmakers and jurists. Such knowledge is expressed through the semiotic concept which evaluates if a writing system is capable, in practice, of asymmetric concealment. If it is, one's capacity to produce unique personal marks over bit sequences is hidden at the same time that other's capacity to verify their legitimacy is openly revealed. We take note that such writing systems already exist, provided that new levels of acceptance for the meaning of "*personal*" are clarified by jurisprudence, since the intermediation of software and hardware for the issuance and verification of these digital marks is inevitable.

To put this knowledge into perspective, we offer a metaphor with the concept of airplane, once a desired abstraction just like signature on bits now is. The concept of airplane emerged from the observation of birds. It labels, or classifies, those systems of physical transport across the air which are heavier than air. The only possible way to realize it is through the concept of "*wing*" (helicopter's main propeller functions as such). Rocket, balloon, and other intergalactic or telepathic transport mechanisms yet to be invented, are different concepts. In likeness, we want to consider the transport of trust-in-meanings: authentication. In our metaphor, the ground is like the paper's surface, made of cellulose, and the air is like a global digital network, made of bits: today's Internet. The concept of digital signature originally emerged like that of airplane, by abstraction. From observation of what a handwritten signature does on paper. As a process, one of the most important things it does is to give the signer some control over the difficulty of its forgery, this control being the foundation of non-repudiation in contract jurisprudence. In

likeness, if a digital authenticator would allow such control, it would do signatures on bits. If not, it would do something else.

The Birth of a New Concept

The early architects of cyberspace came to the conclusion that the only way a signer can control the difficulty of forgery through manipulation of the signature verification mechanism in a hostile virtual environment, is for him not to have to share the secret he necessitates for producing his personal and unique mark in digital documents. For lack of a better term, we will refer to this use of a writing's asymmetric concealment as "*self control over forgery*". Thus, in a pioneer and seminal article published in 1976, Diffie & Hellman laid down the conceptual framework for authentication systems with self control over forgery, namely, asymmetric or public-key cryptography [9] (it is believed that the military had already arrived at, but did not divulge it). Less than two years later, Rivest, Shamir & Adleman published their discovery of the first of its effective and openly known systems, and still in use, the RSA [10]. Their discovery permitted the realization of the concept of digital signature, as desired. And so they called it [10]. To this concept, asymmetric keys are like wings for airplanes or zeros for calculators.

We shall acknowledge, however, that this has nothing to do with the type of transportation for trust-in-meanings one may choose in cyberspace. There will be several available, just like train, ship, airplane, balloon or rocket in our metaphor. If one wants his trust to preserve the control a signatory may exert over the difficulty for forgery of his signature, as occurs through signing on paper, one has to choose adequate means for transporting that trust through bits. The fact that there will be only one type of transport available in this case, follows from the choice of the kind of trust one wants transported. The fact that asymmetric keys for authentication represent, if one wants to have such specific kind of trust in bits, the same as wings for airplanes and zeros for calculators, follows from the interpretation, pointed to by Diffie & Hellman, of theorems in the mathematical theory of information, proved in 1949 by Claude Shannon [11].

NEW ACTORS, NEW SCENES

Digital or Electronic?

Meanwhile, opportunities for electronic commerce brought new actors to stage. They appropriated a broader virtual meaning for "*signature*", baptizing any digital authentication method as "*electronic signature*", and began spreading confusion they may believe will benefit them. They are marketers, lobbyists and agents with their discourses on technology, using a strategy most favored by the software industry -- their patrons -- known as *fud* (fear, uncertainty and doubt). To these new actors, the original concept of digital signature is only one among possible technologies, one that may become insecure tomorrow [1]. Rather cavalierly, they allowed Rivest et. al.'s concept to keep its original title (digital signature). After all, adjectives are plenty, and their game plan was to deal with a bigger thing, the electronic signature stuff. They spurn or ignore the public-key prescription for digital authentication with self control over forgery, from information theory. They act as if it is just overrated technology, about to be outdated, headed for oblivion. And that what we need now are electronic signature laws that let the market sort things out. They want us to believe all this.

However, that self control quality of authenticators stand as cornerstone for today's commercial law jurisprudence, holding the balance among risks and social responsibilities for contracting parties. Therefore, new laws empowering

mechanisms for signatures over bits are expected to address the question as to whether or not society is to retain such jurisprudence. And if not, why. To answer it, adjectivations of what a dictionary may say under "*signature*" will not suffice, be it with "*digital*", "*electronic*" or "*virtual*" legal terms, since for these laws the thing where signatures must be written on, will be non-physical (bits). And in so being, the signature's quality of originality implicit in said "*written by himself*" loses its physical support and is dissolved by the extra quality of being ethereal, thus creating a new semantic vacuum of deep ambiguities.

Tectonic Ambiguities

Such lexical ambiguity is indeed dangerous, for it is of the same kind set up by the monotheist definition of god, which gives fanatics from varied monotheist religions ammunition for ideological wars over its meaning. Likewise, the meaning of ethereal legal signatures and of cryptographic functions have become war horses for ideological control of the digital revolution, in which new freedoms threaten old powers and new powers strangle old freedoms. Those who trade in coins having technology engraved as head and virtuality as tail must take heed. It would be naive to believe, and foolish to suggest, that a camouflage of these semantic conflicts in thick legal jargon can be permanent or effective, while this camouflage would be only protecting a time bomb. The new signature laws modeled after the UNCITRAL proposal, as well as some DMCA provisions, are in some sense similar to Florida's electoral statutes, in that their ambiguities lay precisely over faults in tectonic semantic plates, built from symbols. Moreover, the new juridical cyberscenario seems potentially worse than Florida's electoral statutes, because its geology has been obfuscated by *fud*.

It would be indeed naive and risky to disregard the danger in granting the signification of "*unique and personal virtual mark*" to parts involved in the balance of interests and social responsibilities under common law, as has happened to the signification of "*voter's clear intent*" in Florida. The model proposed by UNCITRAL suggests that new signature laws shall keep their authentication concepts to their lexical surface, ignoring the consequences of ensuing deep ambiguities. The grant issued by laws like those have in common the fact that what begs signification are human volitive acts, intermediated by machines, where the law is ambivalent over whose and which judgment shall prevail through arbitrage. And how.

UNCITRAL's Gordian Knot

The UNCITRAL proposal handles its doctrinaire philosophical implications in a manner similar to Alexander the Great before the gordian knot. It suggests "uniformization" of worldwide arbitration jurisprudences through their radical reversal. In article 13 of "UNCITRAL Model Law On Electronic Commerce With Guide To Enactment", it is recommended that these laws shall put the burden of proof of forgery or due care on the alleged signatory, reversing juridical traditions almost completely and clashing with code in place, such as the Electronic Transactions Act (CWTH) of 1999, whose section 15 rejects UNCITRAL's article 13 and determines the imputability of digital signatures only through express consent of the alleged signatory. Both provisions err in unbalancing risks, in opposite directions [5]. This UNCITRAL's gordian knot arbitrage solution for laws permitting authenticators in which signatories have no control over forgeries, is not some fictional conspiratory theory. It is indeed written in an United Nations' legal commission's recommendation. [12]

Whatever the provisions in such laws may be, on rights and due process in arbitrage over signature repudiations, these laws will

be flawed if the reliability and trustworthiness of the computational environment producing and verifying digital signatures can not be demanded and asserted. And here, beyond the technical difficulties related to public confidence on such trust assessments, explosive material for the electronic signature's time bomb is fabricated. Wrapped in legal lexical ambiguities, the explosive formula mixes, on the one hand, the need and the means for those trust assessments, and on the other, the jurisprudence being formed on intellectual property rights of software producers. Needless to say, the ensuing conflict will bring great insecurity to citizens and opportunity for lawyers. But suitable to say, it would be a folly for lawyers to disregard their own citizenship condition from all this.

THE CHOICES, BEHIND AND AHEAD

Waving Promises

The legal adjectivation of terms with complex meanings, such as "*unique and personal mark*", has to be carefully planned, for the new quality may clash with those defining the term. For instance, wouldn't a unique (and thus supreme) god have the power and discretion to share his/her own godness? What this only god might be, may seem clear on the surface, but not in the Middle East, where wars have been and are being waged over it. Likewise, what a digital or electronic signature might be, may seem clear on the surface, but not in cyberspace, where battles will be waged over its meaning. And the longer these battles are postponed, the worse their violence will be, even if symbolic.

Unlike airplane and decimal system, the concepts of "*unique god*" and "*electronic signature*" are not sedimented in our cultures. Therefore dictionaries will not help us -- including judges and regulators -- understand their meanings. The alleged superiority of the grant model, anchored solely on waving promises of wonders from technological progress, is a farce that needs to be denounced if thinking people, not thinking money, are to decide the kind of digital signature laws society may have.

Semiotic Prestidigitation

In preliminary skirmishes over the meaning of digital/electronic signature, quick shooters are lobbying for the legal empowerment of authentication systems in which the signatory has no control whatsoever over forgery [13]. In times when we should all beware of the consequences of humans losing control over the meaning of their own actions amidst the digital revolution, these semiotic prestidigitators distract our attention by waving threats posed by lamers and script kiddies, while juggling digital/electronic adjectivations. The role, in the ensuing debate, for a cryptographer who has social duties in his job description, is to offer his understanding about the extent and means by which essential qualities of handwritten signatures can be replicated in cyberspace, and the texture of underlying uncertainties from such replication. But this role is tough, because *fud* strategies for hammering the neutrality argument against prescriptive legislation explore uncertainties with deep pockets and machiavellianism.

Their mantra says that public-key technology (in the singular!) can become insecure with technological progress, or with upgrades in computational power available to scoundrels. Such litany ignores the fact that all of the known public-key technologies can adjust the cost of algorithmic attack against them through key size parameters at key generation, and that such capacity has been used for over twenty years. It despises the fact that, for the least sophisticated of these technologies to become obsolete, yet unknown algorithms able to escape such

cost control capacity would have to factor integers efficiently, whereas such algorithms have been sought by the most brilliant mathematicians for millennia, to no avail. The argument that tomorrow we may have some bad surprises, and therefore we should let the big smart boys tell us what is best for us today, sounds as coming from George Orwell's "1984".

Conclusions

We believe to have collected enough evidence for prudence yielding at least two prescriptions for new signature laws. One for the use of asymmetric cryptography in authentication technologies, for contexts where signatures in digital media are to register human intent or consent. Negligence at this will transform the arena where the meaning of new signatures is left to be decided, in a battleground where powerful players will impose theirs. With the aggravation of their immunity from responsibility and risks, inevitably driven to citizens. Another prescription is yielded for establishing, as a condition for legitimacy of these technologies, that public access to the inner logic of protocols and software deployed to generate and verify keys and signatures shall not be hindered by any intellectual property right or license provision. Its negligence will give judicial systems a quicksand foundation for developing jurisprudence on arbitration, making the Florida 2000 presidential election imbroglio look like a mere academic exercise.

The only possible technical or political explanation left for the success of the grant model seems to be economic. This is plausible, because the known technologies of asymmetric cryptography happen to be in public domain, already settled on open standards and even deployed through open and free software. There will be no justification for extra costs with patents, market domination struggles or non-disclosure demands in implementations of public-key technology. All compelling reasons for it to look bad to the logic of greed, and to look good to the logic of human freedom, corroborating our early crossroads claim. After the advent of alphabets, no human language seeking written expression has spurned them. After the advent of zero as concept for positional numeric writing, all civilized accounting practices ended up adopting its systems. For the simple and final reason that they are functionally far more advantageous than their possible alternatives. The Romans resisted more than 300 years to adopt the decimal system, introduced in Europe by the Arabs, but were finally subdued by galloping inflation. They were victims of a noise similar to what we hear today around the word *technology*, for they would not admit that "insignificant people" could come up with something smarter than they could.

Those who defend the grant model seem unable to see the fallacies in their own arguments, as pointed to by prescriptive model advocates. These fallacies are neutralized, by laws held superior to laws of reason in the semantic referential from which they perceive the world. Those of the market. As then in Rome, energumen of today are reluctant to admit that discoveries of asymmetrically concealable writing systems, by mathematicians who availed themselves of 2350 years of their science's legacy, could represent a qualitative leap in relation to what entrepreneurial creativity is able to foster for the collective security in an open and global digital network. We are left wondering what the social cost for acceptance of this fact will turn out to be. This cost will be charged by the arrogance and greed of a powerful few, who see themselves as cunning. Are we prepared to abdicate the "collective" in the security of cyberspace and retrocede to barbarity, in exchange for the collectivization of greed, as is already happening in the live

world, at the fringes of the new economy? Can cyberspace be secured, if not collectively? Can we learn the answer from earth's environment? Or perhaps the biblical book of Revelation holds the key for the script at play, in its verse 17 of chapter 2? These are questions this article wishes to proclaim as crucial.

BIBLIOGRAPHY

- [1] R. M. Nunno: "*Electronic Signatures: Technology Developments and Legislative Issues*" CRS Report for Congress, working document. Congressional Research Service - The U.S. Library of Congress. Accessed Sep 2000.
- [2] C. Meadows: "*A survey of formal methods for criptografic protocol analisys and design*". 1999, SRI Research Institute
- [3] L. Weinstein: *PFIR Statement on Electronic Signatures and Documents* <http://www.pfir.org/statements/e-sigs> (Dec 9,00)
- [4] L. Lessig: *Code, and Other laws of Cyberspace* 1999, New York, Basic Books
- [5] A. McCullagh & W. Caelli: *Non-repudiation in the digital environment*. F. M. Electronic journal (Dec 9, 00) http://firstmonday.org/issues/issue5_8/mccullagh/
- [6] J. Seberry & J. Pieprzyk: *Cryptography. An Introduction to Computer Security*, 1999, Sidney, Prentice Hall . pp 88
- [7] U. Eco *Tratado Geral de Semiótica* Translation from *Trattato di semiotica generale*, 1980, São Paulo, Perspectiva
- [8] Webster's New World Dictionary, College Edition 1955, New York, The World Publishing Company
- [9] W. Diffie & M. Hellman: "*New Directions in Cryptography*" IEEE Transactions on Information Theory, IT-22, Vol 6, Nov 1976, pp 644-54
- [10] R. Rivest, A. Shamir & L. Adleman: "*A Method for Obtaining Digital Signatures and Public Key Cryptosystems*" Comm. of The ACM Vol 21, No. 2, Feb 1978. pp 120-8
- [11] C. Shannon: "*Communication Theory of Secrecy Systems*" Bell Systems Technical Journal Vol. 28, 1949, pp 656-715
- [12] *Uncitral Model Law on Electronic Commerce With Guide to Enactment*. United Nations, 1996. (Dec 9, 00) <http://www.uncitral.org/en-index.htm>
- [13] *Advogado da Microsoft Critica Governo Brasileiro* <http://www.canalweb.com.br/noticias/noticia.asp?id=447> (june 29, 00)