Global relevance of the European Electronic Signatures co-regulation process

Recent studies have made clear that software and hardware have in themselves a regulatory capability which stems out of their nature. The binary system/logic is a high hierarchical structure which utilises norms to rule its dynamic processes.

It is also in every day's life obvious that abilities and inabilities of software and hardware that we utilise, affect in very direct way human life and the ability of users to choose freely how to act.

IT has so an influence on human life. Despite it is a social and economic phenomenon, it seems quite immune from human regulation, as it would be a natural process.

There is a clear conflict between IT self-regulating ability and state regulation, which is easily perceivable through the apprehension one can feel in front of an Automatic Teller Machine (ATM) when it comes the moment when cash should be dispensed, or through the concerns raised by last innovations in the area of operating systems (e.g. Windows XP, where the software for the needs of its functioning -and maybe also for the protection of copyrights of its producer- brakes into the undisputable individual freedom to change configuration of a PC's hardware).

From the most trivial to the most complex conflict between individual freedom, rights of industry (or intellectual property holders), it is clear that software and hardware do not only cause regulatory problems, but are by themselves regulatory tools. And it is also obvious that the regulatory capability of such products, has an impact on the day-to-day life, which can sometimes be more perceivable than rules set by state regulators. The discussion on the Microsoft Passport technology is a blatant example of this situation.

How to solve this conflict of norms? How to co-ordinate rules coming out of the technical features of objects (or products, or systems) and the rules provided by the regulatory system of our society ? Until the spread of Internet, as a fundamental network of communication and information diffusion, there was only one obvious answer to the question above: the regulatory powers of the state were, from the formal perspective, in a pre-eminent position and had not only the right but also the possibility to require changes to technology which was not complying with the ruling of official norms. So it happened in regulating electricity, where the required security features, were different in each state, and so the plugs, the voltage, or other technical components/features.

Since IT has become global and it is utilised more or less everywhere, the reach of national regulators on IT has become significantly weaker, if not existent at all.

On the other hand self regulatory organisations like those set by the Internet Community (W3Org, ICANN, IETF) have no legitimation to provide rules also expressing the political interest of individuals or entities participating to the Internet Community. In fact their election procedure is not able to guarantee proper representativeness.

The paradox of present time is that, who is able to represent global perspectives is not able to represent political ones and those that have political legitimation normally are not able to represent properly the global point of view on technology and international regulation.

The very generic regulation set by WTO and OSCE in the field of open networks, Internet or IT Security are there to demonstrate that a political compromise which is aimed to be somehow global, risks to be completely empted of content and regulatory capability. This is maybe because this so called international political panels and organisations are mainly composed by official state representatives which, in that context, generally represent the political point of view of the national government and not, like it happens (for an instance) in European Parliament, the different opinions and political perspectives which is possible to find in each of the countries represented in such international panels.

This is not to say simplistically that a "world parliament" would be the right place where to regulate Internet. But it explains, why probably such international organisations which try to deal with the phenomena of Internet and open networks are until now, even if provided with political legitimation, unable to produce an effective and up-to-date regulation of open networks and IT security. They have an approach which is not truly global. It is a negotiated compromised between national interests, made looking at national situations.

Is it possible to be free in a space in which technical self regulation is not able to solve political problems and politically representative organisations are not able to deal properly with technical problems which have political relevance? How free are human beings living in a society in which there is no possibility to express in a structured way their interest within a certain context ? Makes it any sense to be Robin Hood forever ?

On the other hand, how compatible are to our political and economic system, regulations on IT security which prohibit digital self-defence or enable state prosecution to ignore privacy and the right of legal defence ? Can they co-exist with the effort to spread utilisation of digital documents in legal relevant transactions and for government?

The questions above, show that possibly one has to look at the present situation as some kind of the prehistoric time of Internet. In fact, as in pre-historic societies, individual interests can be only composed through fight, because there are no other accepted procedures to do so.

We have a legislative prehistory.

Legislator is tempted to fill the vacuum with draconic regulation, in the attempt to achieve control of the situation. But each national legislator is doing so in a different way, de-legitimating themselves in front of the international community. Users, feel the attempt of state bodies to interfere with the sphere of their individual rights, as they have been granted to them until now (there was no attempt to prohibit encryption of private communication, before telephone and Internet). In a society which bases a relevant part of its wealth on advanced services, it is strange to see the legislator trying to limit quality and security of possible services. It is strange to see that fundamental individual rights granted in real world, should be erased in the cyber-world, according to many police enforcement bodies.

Any attempt of the state regulator to impose key recovery or to prohibit digital security (limiting freedom of cryptography), is a middle-age obscurantist approach to regulation. History shows that torture for law enforcement, cruel punishments for criminals, deletion of individual rights were not able to preserve a society which was poor because it was living in fear. Western societies are opulent, wired and based on trust. Western societies cannot stick to prosperity, if the rule of law has to be achieved through the infringement of individual freedom.

Moreover, any try to limit individual rights would affect only honest citizens. Criminals would just ignore such regulations and use cryptography or any other forbidden mean to achieve his/her goals, if the punishment for using cryptographic tools is lighter then that provided for the crime to be hided. Only illiberal societies provide higher punishment for the try to hide the evidences of a crime, then for the crime itself.

Are legislators (in good faith?) regressing (because of ignorance?) to prehistoric law enforcement policies ?

There is also an organisative prehistory.

Organisations like ICAN, W3Org, IETF look more like the effort of the very ancient Greeks to build the Polis (before the Polis was there, with its set of politically and socially agreed rules) than like a Polis itself. No representativeness is already recognized/organized. The factual legitimation has not already created a regulative framework. In fact, efforts to bypass the Internet self-regulation are made by the legislator of different states (China, USA, France, etc.), as well by Industry, trying to strengthen de-facto monopolies or other (mostly national) privileged positions.

Such statements do not try to de-legitimate the present process of self regulation, which is absolutely necessary and scoring much better then any attempt made by monopolist industry or legislatorn, with the sole exception of the European Directive on electronic signatures (93/1999/EC), as we will see.

This kind of statements, try to put in a relative timeframe what presently is done. and to show its fluidity. The dynamic aspect of the present situation is that technical and political legitimation are somehow coming together, to find a possible way to deal with technical and political/legal problems of IT security and open networks.

The European Union with the so called co-regulatory approach to the electronic signature has tried, possibly, the first effort in the direction to bring together the political and the technical world in a structured way, respectful of the needs and the dynamics of each of the two worlds.

With the 1999/93/EC Directive, the European legislator has defined a set of goals to comply with, to make electronic signatures and digital documents equal to paper-based documents provided with handwritten signatures.

This equivalence, which was for the first time introduced in a legislation in Italy in 1997, with the so-called Bassanini Decree, makes possible to organise public administration and private administrations in a more paperless way, because also formal contracts or any kind of deed which needs handwritten signature can be substituted with the full equivalent in digital form.

What the European legislator did not (and very consciously indeed) was to define the technical means to achieve such ambitious goals. For the definition of the technical means European Directive refers to existing standards.

In fact, all technical standards relevant for

a) security of cryptographic modules,

b) security of trustworthy systems and

c) security of Secure Signature Creation Devices (SSCDs)

shall be referenced by a Committee set up with national delegations of the member states, accordingly to Art. 9 of the 93/1999/EC Directive (the so called “Art. 9 Committee”), if the technologies are secure enough to allow a qualified signature to be as safe as a handwritten one. So, Article 9 Committee, is not able to produce any kind of ruling of definitions because it has to work and to reference only with existing standards.

In this way European Directive tries to be technologic neutral and tries to leave to private and industry the definition, the management and the improvement of standards and technology needed for security of electronic signatures.

To complete the regulative process, the European Union has:

a) set up an international panel of IT experts, to co-ordinate the different standardisation initiatives: the European Electronic Signature Standardisation Initiative (EESSI)

b) committed to the European Committee for Norms (Cen) and to the European Telecommunication Standardisation Institute (ETSI) the technical management of two open standardisation workshops. These are “Cen-ISSS E-Sign” and “ETSI ESI”.

The workshops produce so-called pre-standards in the form of Cen Workshop Agreements (CWA) and ETSI Technical standards (ETSI TS), for the reason that formal standardisation procedures are too slow to cope with the pace of technologic innovation. Such an approach has been notoriously successful in defining the GSM standard.

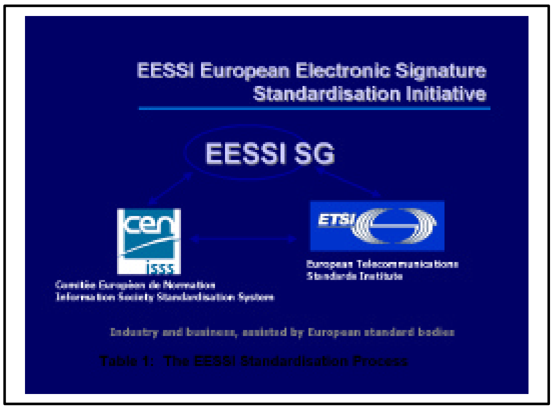
EESSI European Electronic Signature Standardisation Initiative
EESSI SG
cen
isss
Comitée Européen de Normation
Information Society Standardisation System
ETSI
European Telecommunications Standards Institute
Industry and business, assisted by European standard bodies

Table 1: The EESSI Standardisation Process

Table 1 shows the structure of the standardisation process.

The standardisation process which the European Community funded and structured within the existing international standards organisations (ETSI and CEN) has chosen the most global system of IT Security assessment which is presently available, which are the Common Criteria to define the protection profiles of the targets of evaluation.

In doing so, not only in Europe, but also in the rest of the world it is possible to assess and to verify the compliance to IT security criteria of devices and systems utilised for producing electronic signatures. This then more necessary, considered that US and Asian Certification Service Providers (CSPs) are eager to see their products/services recognized as EU Directive compliant.

Looking to this process from a functional prospective it is possible say that the European legislator, setting the goals and not defining the tools (or the means) through which to reach such goals, was passing the problem over to the industry and privates. Because, to assess security of PKI technology, the EESSI standardisation process has chosen an international IT security assessment system, which is presently mostly state led, to preserve the co-regulation process, it seems recommendable, that the Common Criteria management system, starts to open itself more to the participation and to the inputs of privates.

This is relevant, as shown in the Table 2, because to improve a cyclical legislation, it is necessary that the allowed implementations are enough defined by industry practices. Otherwise the (European) legislator will receive very feeble imputs in order to improve existing regulations. The balance between different needs/approaches will be found at an administrative and not at a political level. In this case, co-regulation would not be a new thing, because the participation of privates to administrative processes is common practice since more then 30 years, in advanced democracies. The really new approach is to involve privates in defining the detail of norms set at highest political level. Today, only this innovation seems to be able to provide political endorsement to technical standards that impact on aspects of day-to-day life of most part of the population. Anyway, this co-ordination is at a first stage and not already perfectioned.

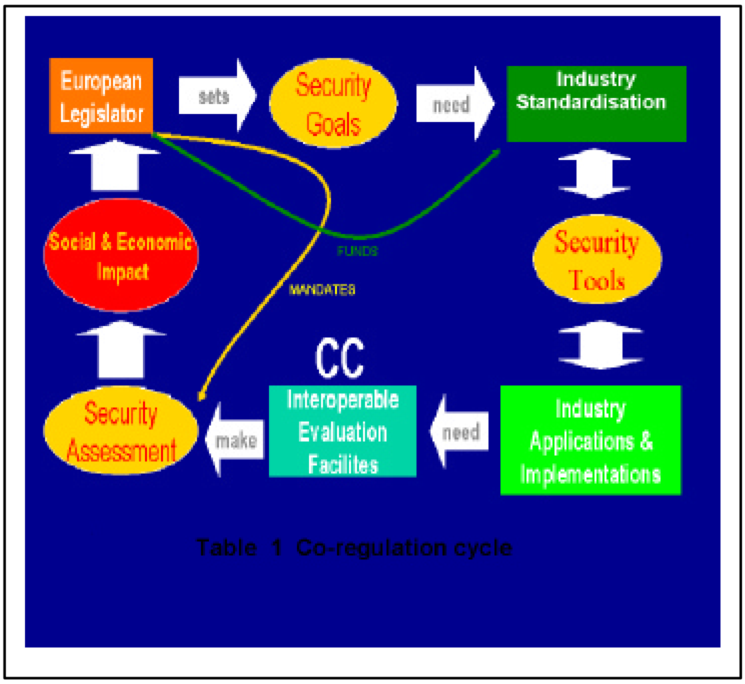

Table 1 Co-regulation cycle

In fact, looking to the German experience, it is possible to fear the risk of a kind of short circuit of the process. The Protection Profiles of the Secure Signature Creation Device have been approved by the European Electronic Signature Standardisation Initiative (Cen CWA 14168 and CWA 14169), with the contrary vote of the national supervisory body (Regulierungs-behörde für Telekommunikation und Post –RegTP-). Such Protection Profiles, are currently evaluated by TÜV-IT GmbH (a German IT security evaluation facility). At the end of the evaluation, it is necessary the verification of the evaluation process through the national Common Criteria accreditation and verification body, which is the Bundesamt für Sicherheit in der Informationstechnik (BSI), also involved in making the standard. RegTP and BSI are both part of the German national delegation of the Article 9 Committee, which according to the Directive 93/1999/EC has to reference the standards which have to be accepted by each member state. It is possible to see that the same administration intervenes in the co-regulation process, with different roles, in a manner that is not functional to the process, and gives to such administration some kind of privileged position (to some extent inconsistent with the claim of co-regulative approach).

The situation in Germany, is even not worst case scenario: what happens, in fact, if the national Common Criteria accreditation and verification Body is strongly opposed to a certain Protection Profile, approved by the standardisation process ? It could be too optimistic to rely on the fact that the verification procedure of a Protection Profile is just a formal/technical one. And if such short-circuits will occur, there is the risk that the international standardisation process will refer not to Common Criteria but to other (less global, but more industry led) IT security assessment schemes. A worst case scenario, that should be avoided.

In conclusion, it is possible to consider the co-regulation approach of the European Directive 93/1999/EC a first great step in the right direction. Even if the mechanism of co-regulation, as structured now, is not already able to guarantee a truly cyclical co-regulation process, anyway it is a start that allows to have first co-ordinated inputs of regulation and self-regulation to the market players.

This model, if adopted by also other regional supranational organisations like the Asian SEAN or the NAFTA (between US, Mexico and Canada) or the MERCOSUR (Latin America), it could become a first step in the direction to find the process which is able to represent in the regulation of IT security and open networks not only political and not only technical aspects but, in a coordinated way, both of them, not only from a purely governmental point of view.

The existence of different co-regulative approaches can only have a positive effect on their fine-tuning.

According to the assumption of this paper, it is clear that an improvement of this co-regulation process is not in the hands (only) of the European legislator. Also IT security assessment organisations and industry shall become aware of the global relevance of this approach and re-define their processes and goals accordingly.

There are good signs in this direction, but not already enough awareness to be sure that the co-regulation approach will succeed in a way that most national legislators and industry will adopt it. Are there around any better alternatives ?

Dr. Riccardo Genghini
Chairman of
Cen-ISSS E-Sign Workshop
on Standardisation of Electronic Signatures