Journal of Modern Accounting and Auditing, ISSN 1548-6583
November 2013, Vol. 9, No. 11, 1469-1482

Impact of International Networks on Standardization Process in Banking Industry: Example of Secure Electronic Transaction (SET) Initiative

Paul Marc Collin
University of Lyon 3, Lyon, France
Hana Machková
University of Economics, Prague, Czech Republic

The purpose of this article is to present and interpret the case study of the secure electronic transaction (SET) scheme of Internet security, as an illustration of the necessary construction of interoperability solutions for financial services. The interpretation of case data with actor network theory (ANT) provides an illustration of power coalitions among banks to create a *de facto* standard for transnational electronic payment security on the Internet. After a step of protecting its political interests and well-known technological solutions, the coalition understands that its mission becomes a matter of life and death for its members: Brand-new currency has been invented on the Web and one could develop business and monetary transactions without the banks. This interpretative stage tells us much about the transnational mechanisms of regulation and standardization as well as the "translation" steps regarding these transnational organizations. However, an additional step has to be added to this interpretative step, a step of framework construction. The aim is to help managers of the transnational firms involved in regulations and standardization to anticipate the evolutions and make relevant decisions. The framework has three distinctive characteristics: the ability to help conception, the ability to help conceive problems "ex ante", and the ability to facilitate collective conception of strategic maneuvers.

Keywords: cyber payments, bank cards, deterritorialization, financial markets, secure electronic transaction (SET) specification

Introduction

One of the most striking phenomena of the past decade has been the internationalization of service firms. Previously considered "un-exportable" (Machková, 2009), they have proven day after day that they have the necessary characteristics to undertake an international development, and even a globalization of their offering systems (Campbell & Verbeke, 1994; Gadrey, 1994). Retail banking and financial services are remarkable illustrations of this phenomenon and bank cards in the first place (Collin, 2006). The field study selected for this article is relative to the bank card organizations, the development of international standards bodies, specifically in the area of Internet payments and the construction of a transnational regulation.

Paul Marc Collin, associate professor, IAE, University of Lyon 3. Email: paul-marc.collin@univ-lyon3.fr.
Hana Machková, CSc., professor, Department of International Trade, Faculty of International Relations, University of Economics.

The detailed case study presented and interpreted is the secure electronic transaction (SET) scheme of Internet security and its localizations in multiple countries of operation. Interoperability is questioned in the context of industry globalization. The role and behavior of transnational agencies such as CyberComm are scrutinized. One of the originalities of this paper also lies in its epistemology and methodology. After a phase of interpretation of case data through the translation theory (Callon, 1986; Latour, 1989; Czarniawska & Sevon, 1996; Sahlin-Andersson, 1996), the authors undertake a step of "framework" construction (Porter, 1991; Claveau, Martinet, & Tannery, 1998; Folger & Turillo, 1999; Tsoukas, 1996), in order to offer managers an "ex ante" strategic decision tool. The translation school seems to offer a sensitivity for hybrid methodology (content and process), very useful for the analysis of transnational firms. The introduction of the notion of "actant non-human", the technical object which builds socio-technical networks, has enormous potential in management science. This concept includes all the stakeholders of transnational networks of standardization.

The authors have then started with the interpretation of case data with translation theory concept in the frame of transnational bankcard networks, for example, a coalition among banks to create a *de facto* standard for transnational electronic payment security on the Internet. The case study is eye-opening. After a step of protecting its political interests and well-known technological solutions, the coalition understands that its mission becomes a matter of life and death for its members: Brand-new currency has been invented on the Web and one could develop business and monetary transactions without the banks.

This interpretative stage, while broadening the horizon and the relevance of observations, has taught the authors much about the transnational mechanisms of regulation and standardization as well as the "translation" steps regarding these transnational organizations. However, an additional step has to be added to this interpretative step, a step of "framework construction" (Porter, 1991). The aim is to help managers of the transnational firms involved in regulations and standardization to anticipate the evolutions and make relevant decisions. The "framework" has three distinctive characteristics: the ability to help conception, the ability to help conceive problems "ex ante", and the ability to facilitate collective conception of strategic maneuvers.

Presentation and Genesis of Internet Payments (Cyber Payments)

In this article, the authors will deal with the concerns around cyber payments and their impact on the emergence of transnational regulation. What are the challenges of cyber payments? Cyber payments are an emerging new class of instruments and payment systems that support the electronic transfer of value. These transfers may take place via networks, such as the Internet, or through the use of stored-value type smart cards. Because of the efficiency and ease with which they transfer value, these systems may also present new challenges to law enforcement. Technology exists which could permit these systems to combine the speed of the present bank-based wire transfer systems with the anonymity of currency. As a result, there are issues that must be addressed, as these systems are being developed to ensure the prevention and detection of money laundering and other illegal financial transactions.

Internationally, cyber payment systems have also received extensive attention. Multilateral discussions and studies have been undertaken by both the G-7's Financial Action Task Force (FATF) and the G-10's Working Party on Electronic Money. For example, in June 1996, recommendation #13 was added to the FATF's 40 recommendations. It states that countries should pay special attention to money laundering threats inherent in new or developing technologies that may favor anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

What is the current state of cyber payment technology? Progress toward technical and commercial standards in the cyber payment industry has been steady, and the emergence of cyber payment systems is gathering momentum. A number of stored-value type smart cards and network-based products have undergone pilot testing. These tests have taken place on a global basis, thus underscoring the international nature of the emerging cyber payments infrastructure. Some cyber payment instruments' features, such as peer-to-peer value transfer and payer anonymity, offer consumers an instrument with much of the flexibility and convenience of cash together with an enhanced ability to conduct purchases on an almost global basis.

This technology suggests that law enforcement must begin to consider the potential implications of an environment where the wide availability of cyber payments instruments could substantially reduce the use of physical currency in consumer-level transactions.

The market potential seemed tremendous, and the global usage of new technologies was conditioned by two main factors: standardization and network cooperation. The Europay-MasterCard-Visa (EMV) for example was working on joint standards for smart card protocols to be used in electronic commerce (Dvořák, 2005). These smart card efforts go beyond the many methods that are being discussed that allow for secure credit card transactions over open networks, such as First Data's joint program with Netscape Communications Corp.. First Data, a credit card transaction processor, has a system that encrypts credit card numbers for customers making purchases on the Internet.

The pursuit of a *de facto* standard accessible to the entire profession operates as a signal that the major players were eager to create a common good for the industry. However, it is noticeable in our example that they use this opportunity to act as partners with their competitors to impose their technological solutions (Callon, 1986), namely, the use of the smart card technology. Hence, this "translation process" (Callon, 1986; Czarniawska, 1996) could be analyzed as a means of "recycling" existing technologies in techno-political projects with high visibility and potential marketing gains for each of the networked organizations. Subsequently, opportunistic pilot projects help "discipline" the stakeholders (suppliers, customers, and national public authorities), while actual physical deployment (including ATMs[1] and EFTPOS[2] materials) provides the basis for durable networking and standardization.

In terms of innovation process, the authors could propose the following typology: When analyzing the range of electronic commerce propositions, it may be useful to further categorize them as either "technology extensions" of current financial practices, or alternatively, as true electronic cash, although it is not always simple to make the distinction. Technology extensions can be thought of as tools and technology that allow us to operate the present financial instruments of checks and credit cards more quickly, securely, and accurately. Beyond the enthusiasm, the authors observe a growing concern around the issue of security of payment.

Trend Toward Deterritorialization: Cyber Payments in the Cyberspace

The first dimension of the cyber payment concern relates to geopolitics and globalization. We are told that we face an era of radical changes. One of them is the "deterritorialization" (Toal, 1999). Quoting Virilio and Lotringer (1983), it could be said that, beyond some words like globalization, translocality, glocalization, transnational, and cyberspace, what is being described is the re-arranging and re-structuring of spatial relations as a consequence of the technological, material, and geopolitical transformations of the late 20th century.

[1] ATM: Automated Teller Machine.
[2] EFTPOS: Electronic Fund Transfer at the Point of Sale.

To speak of deterritorialization in contemporary discourse, according to Toal (1999), is to speak of a generalized dismantling of the complex of geography, power, and identity that supposedly defined and delimited everyday life in the developed world for most of the 20th century. It is to speak of a new condition of speed and "informalization", of the transgression of inherited borders, of the transcendence of assumed divides, and of the advent of a more global world. Though regimes of territoriality are constantly in flux and under negotiation, discourses of deterritorialization tend to ascribe a unique transcendency to the contemporary condition, defining it as a moment of overwhelming newness.

Economically deterritorialization is held to be a consequence of an unstoppable globalization of previously discrete national markets and economies. In Ohmae's (1995) idealized world, multinational companies are truly the servants of demanding consumers around the world.

Deterritorialization and Financial Markets

One of the traditional markers of state sovereignty and territorial power is the ability of a government to print its own money and control its own financial destiny. But since the break-down of Bretton Woods, the state territorial character of financial markets has been thrown into question. Transnational corporations were forced to develop their own foreign exchange departments (Taušer, 2007). Financial services companies became increasingly important to the conduct of international business and trade. The Bank of England allowed British banks to take deposits and make loans in dollars in 1958. The London subsidiaries of American banks were also allowed to do this. The Eurodollar markets began to grow, because they were not subjected to the same reserve requirements and interest-rate restrictions as national markets and financial institutions. Another important development was the deregulation of financial markets in the late 1970s and 1980s. A third development was the introduction of information technology into finance. Online transaction processing, electronic wire transfers, automatic transaction machines, and electronic data interchange radically altered the space-time relationships governing the financial sector, integrating regional financial markets, encouraging global 24-hour trading horizons, and enabling faster transactional and response time.

The argument was used that global financial integration leads to the end-of-geography, but it seems that one geography is being replaced by another. In fact, the coordinated actions of the G-7 states still set the rules for the world financial system (Hirst & Thompson, 1996). But deterritorialization also operates at a more local level and in a more controversial way. Policies of discrimination and "red-lining" credit exclusion tend to create multiple classes of "financial citizenship" in many states (Leyshon & Thrift, 1997). The authors decided to present some controversial viewpoints to show that financial matters are far from rational in the way they are being socially constructed by the actors. But this rhetoric of newness and revolutionary change needs to be problematized for its overstating of the implicit normalization of technologically deterministic visions of change (Newman, 1998). The risk of technological determinism is always present in the field of regulation of payment systems. Knowing it and selecting a research perspective which plays around this determinism can be useful.

Disintegration of Sovereignty

Discourses of deterritorialization are an attempt at exploring a somewhat neglected issue in contemporary political geography, namely, the long relationship between technological systems and the world political map (Toal, 1999). Driving most contemporary claims of deterritorialization is a "skein of networks" (Latour, 1989),

comprising complex technical systems, from micro-radio-communications and satellite transmission systems to transcontinental optical cable lines (Latour, 1989). This in turn enables everything from e-business on the Internet to 24-hour television broadcasting and deep space navigation. These telecommunication networks have a long history and are much more than tools or conduits for the transmission of information. Rather, they are socio-technical networks. In Latour's (1989) terms, they are "actor-networks" that combine humans and machines in co-evolving arrangements of mutual constitution and dependence. Parallel to the process of deterritorialization, the authors find the process of sovereignty disintegration.

With the Global Information Infrastructure (GII) initiative, for example, territorial borders disintegrate as key paradigms for regulatory governance. Transnational information flows on the GII undermine the foundational borders and erode state sovereignty over regulatory policy and enforcement. Physical borders become transparent and foreign legal systems have local relevance. With electronic cash and new means of electronic stored value, such as those developed by Cybercash and Mondex, Internet transactions may take place entirely on the network without the physical delivery of goods and services and without resort to any national payment system. Yet the GII creates simultaneous global right holders. A given activity may be subjected to differing rights at the same time, such as trademark or antitrust protections, because the activity transcends the borders of any single nation. In addition, the temptations to apply national laws and standards extraterritorially further compound the legal uncertainty.

Network borders have a strong tendency to replace national borders. The visible network borders are contractual ones. For example, the demarcation lines among network service providers such as America OnLine, CompuServe, EUNet, or Prodigy create important boundaries. Network architecture also creates a significant type of border. Gateways among different systems establish fundamental rules of conduct. In effect, technical standards exert substantial control over information flows. Technical standards set default boundary rules in the network that tend to empower selected participants. These visible network borders arise from complex rule-making processes. Technical standardization may be the result of a purely market-driven process or alternatively may be adopted through a standards body. The classic example of a market-promulgated standard is the QWERTY keyboard. Once the now famous keyboard configuration became popular, public acceptance of other, more user-friendly configurations was unlikely. In contrast, standards bodies seek to identify and recommend technical specifications for particular network needs such as security. These organizations, such as the American National Standards Institute (ANSI) and the International Standardization Organization (ISO), play a critical role in the development and promotion of technical standards. In essence, these organizations assure and reinforce the contours of network borders (Reidenberg, 1996).

In addition to the new "geography" of borders, networks may now even supplant substantive, national regulation with their own rules of citizenship and participation. Networks themselves take on political characteristics as self-governing entities. Networks determine the rules of participant behavior. This characteristic can result in rules that reverse established territorial laws. Like nation-states, network communities have significant powers to enforce rules of participant conduct. In the case of proprietary networks such as CompuServe, service providers may terminate access for offending participants. The Internet has the equivalent of self-appointed policemen and policymakers. Spamming, the sending of unsolicited messages, results in "cancelbots", programs that delete messages circulating on the Internet from offending senders. Even collective efforts in adjudication of disputes are likewise emerging in the network community.

There is at least one mechanism, the Virtual Magistrate, for online dispute settlement with network-based tribunals of experts. Although attractive, this device deserves serious fine-tuning.

In this context, we are faced with the incongruity of traditional regulatory policymaking. In the United States of America (USA), for example, national regulators compete with each other for jurisdictional power. In Europe, though, data protection agencies have played a significant role in the formulation of information policy. The European Union (EU), too, has established an Information Society Project Office to coordinate a number of wide-ranging European Commission activities.

The development of a new model for governing networks is crucial for effective policy leadership. The new paradigm must recognize all dimensions of network regulatory power. For global networks, governance could be seen as a complex mix of state, business, technical, and citizen forces. Rules for network behavior will come from each of these interest centers. Within this framework, the private sector could become a driving force in the development of the information society, and governments could be involved in protecting public interests.

Also, the recognition of new network borders opens new instruments for the achievement of regulatory objectives. Standards now contain significant policy rules. The debate over encryption standards and key escrow mechanisms reflects the critical new instrumentality of standards-setting.

Should we recognize network systems as semi-sovereign entities? Networks have key attributes of sovereignty: participant/citizens via service provider membership agreements, “constitutional” rights through contractual terms of service, and police powers through taxation (fees) and system operator sanctions. In effect, network users become stakeholders in transnational political and economic communities. Nevertheless, where networks develop parallel to physical society, traditional governments retain crucial public responsibilities and significant interests. The European principle of subsidiarity could fit a new model of governance, where state governments would not attempt to expropriate all regulatory power from network communities. States can even provoke the creation of network standards, but without interfering with each detailed item. The role of the state could shift toward the creation of an incentive structure for network self-regulation.

A particular law enforcement concern regarding the enhanced ability to move funds is the peer-to-peer payment facility being offered by some schemes. At least one card vendor and several e-cash schemes plan to offer consumers the ability to anonymously transfer purchasing power from one electronic purse to another; such payment transactions would eliminate the need for clearing procedures and may provide no audit trail, providing opportunities for criminal abuse.

Another concern relates to the ability of financial transactions and monetary value transfers to escape from the regulated banking industry where regulators have some level of visibility. The issue of non-bank involvement in the provision of electronic purse services was explored by European Economic Community policymakers. A 1994 report from the working group on European payment systems proposed that only banks be allowed to issue electronic purses. At the November 1994 FATF meeting in Paris, it was noted that laundering operations were spreading outwards from the banking to non-banking sector as launderers become more aware of the various directives, legislation, and conventions requiring banks and financial institutions to follow the standard requirements of identification and reporting. These non-bank institutions, ranging from large to small less-traditional financial intermediaries, are subjected to fewer regulatory requirements and examinations, making them potentially more vulnerable to money laundering.

There are some impediments to the implementation of regulation. Law enforcement faces a difficult dilemma. It does not always have easy access to information about the systems' projected characteristics. Another impediment relates to privacy issues. Some believe that cyber payments should be, in principle, just as anonymous as cash transactions. This creates a dichotomy between privacy and traceability. Indeed, financial transactions and monetary value transfers may escape from the regulated banking industry. Hence, banks should retain some level of control. On the other hand, privacy is a controversial issue. But some experts say that consumers are willing to trade privacy for some benefit-convenience or cost. A subtle equilibrium must be found.

Cyber Payments' Regulatory Initiatives

The authors can cite the G-7 FATF. It is an intergovernmental body which began in 1989. The main purpose of FATF is the development and promotion of policies to combat money laundering and specifically to prevent proceeds of crime from being utilized in future criminal activities and from affecting legitimate economic activities.

Another initiative is the one by the Organization for Economic Cooperation and Development (OECD). It considers that, as a matter of urgency, public and private sector institutions should re-evaluate many of the economic, legal, and political frameworks that currently govern commercial activities and the technological and social environments in which they take place. They recommend regulation of the information infrastructure. According to them, electronic services infrastructures must be permitted and encouraged to converge in order to reflect the rapid convergence of networking technologies employed in electronic commerce applications. They also recommended standardization. The group urges governments to adopt a pragmatic approach that does not discourage the development of widely-accepted proprietary solutions, becoming adopted as if they were standards for electronic commerce, but which nevertheless monitors standardization developments closely to ensure that proprietary standards do not become barriers to market entry or impediments to further innovation.

Sahlin-Andersson (1996) wrote about the OECD and its role as a producer of prototypes. The OECD has been described as an information system, a harmonizing agent, an active disseminator of ideas and ideals, and a driving force and creator of national ideas and ideals. International organizations, such as the OECD, play an important role in directing attention to specific countries, specific phenomena, and specific aspects of developments; they codify, compare, and categorize reforms and changes. In other words, they are important editors of reform ideas and experiences (Sahlin-Andersson, 1996).

The authors will at this stage present one example of translation regulation in the area of cyber payments, more precisely in the effort to secure payments on the Internet. One of the initiatives is the construction of the SET specifications (secured electronic transaction over the Internet).

The SET Initiative

The authors present now an interpretation of cyber payments' issues and solutions in terms of the translation theory (Callon, 1986; Latour, 1989; Sahlin-Andersson, 1996). But what is SET? The SET specification is an open technical standard for the commerce industry developed by Visa and MasterCard as a way to facilitate secure payment card transactions over the Internet. Digital certificates create a trust chain throughout the transaction, verifying cardholder, and merchant validity, a process unparalleled by other Internet security solutions. Software vendors whose products pass SET compliance testing are eligible to display the

SET mark on their products. SET participants are merchants, financial institutions, and promotional sites that utilize or advertise licensed software.

The concepts of systems' openness and of trust chain act as vehicles and metaphors of the necessary cooperation within the network. They pave the way for actors (Latour, 1989) to negotiate commonly accessible solutions. The stakeholders reside in differentiated settings: the merchant on a Pacific Island, the cardholder bank in a large European city, and the network in the USA, for example. Service providers can be traced along this "trust chain", ensuring quality and reliability of data transfer.

Let us present the introduction of a new service, the electronic wallet. As a major step forward in helping its issuing banks to provide secure authentication services to their cardholders, Visa EU today announced availability of the electronic wallet. The service will allow Visa card issuers to provide authentication quickly and with minimal up-front investment, therefore helping to build consumer confidence in electronic commerce and reduce fraud. Bankgesellschaft Berlin will be the first to utilize the new service. For Bankgesellschaft Berlin, the choice was very straightforward. Its managing director of card service stressed, in Visa Informations Press, on October 24, 2000, the commitment to providing cardholders with a high level of internet security. Bankgesellschaft Berlin is one actor of the regulation process, in a way. It comes once the SET specifications have been developed, but participate in what Latour (1989) has called "le rallongement du réseau", a kind of structural "cristallisation" of the network, in order to make it sustainable.

What is the genesis of the SET network? On February 1, 1996, Visa International and MasterCard International announced, with others in the industry, the development of a single technical standard for safeguarding payment card purchases made over open networks. On December 19, 1997, SET LLC (SETCo.) was formed to implement the SET specification. The company is supported by borrowed resources from MasterCard and Visa. SETCo. manages the specification and coordinates efforts related to the adoption of SET as the global payment standard.

In terms of "inscriptions" (Derrida), the SET specification is divided into three books: The *Business Description* gives a general overview of the process; The *Programmer's Guide* describes fields and messages and outlines appropriate processing; and the *Formal Protocol Definition* provides the most rigorous description of SET messages and fields. Inscriptions are powerful instruments to enroll the actors. Inscriptions have a double meaning: one of writing down, a second of recruiting and even enlistment, a military term. There is a dimension of "disciplinary recruiting" in the translation theory, which is compatible with the observation of a standardization process.

The most significant solutions for electronic commerce securization are, according to Haguet's (1996) typology: what can be called digital cash (Digicash, Mondex), direct transactions between client and merchant (SET), and intermediation (GlobeID, CyberCash, and First Virtual).

The diversity of solutions shows that translation processes are occurring on a bilateral and multilateral basis among actors of this industry. However, interoperability seems to be the ultimate challenge. Partial spatial-temporal translations call for new translations, aimed at building a solution accessible by everyone, regardless of the technical configuration of his (or her) access point. As far as Visa and MasterCard are concerned, after having worked "solo" for a while, they decided to work together for the "common good". They realized that the power of their aggregated networks could provide the foundation for building a potentially *de facto* standard. And that is exactly what happened with SET. We must admit that the market penetration for this solution has not been satisfactory so far. Some observers question the operational simplicity of SET. Others

challenge the cost of acquiring a costly card reader for each Internet customer. However, SET exists as one of the proposed solutions. And the pressure of national and transnational regulation (the French law, the European directives, as examples) is very present.

SET exists in the public arena, as a proposed standardized way of reducing risk on Internet payments; but it also exists in the private arena, as a private network which is able to enroll participants, transforming them in members and network "citizens". Let us now discover the participant enrollment/change form: This participant enrollment form must accompany all participation agreements. Upon completion of our enrolment, you will receive instructions about mailing lists, participation meetings, and secure access sites. The SET network goes even a step further. Each new member may participate in the development of SET specifications and protocols. This possibility can be analyzed as a form of organizational politics, through which conception power is being granted and openly distributed to each member, old or new. It can also be analyzed as a type of enrolment process (Latour, 1989). You enroll more participants by showing that you are ready to take their interests into account, which will justify their "detour", their way round through the framework of your specifications.

Private networks have enough influence to impose their solutions. For example, one of the card networks envisioned to prohibit the use of its cards on Internet without the appropriate SET software. But to move from private network influence toward power, private networks need the support of public authorities. For example, in France, Groupement Carte Bancaire tried hard and obtained Service Central de la Sécurité des Systèmes d'Information's (SCSSI, a central public body of the French Administration) authorization to utilize, supply, and export C-SET (Chip-SEC), which add a card reader (Bull CP8) to the initial software while ensuring SET/C-SET compatibility.

One may envision an electronic commerce ignoring state borders within the EU (Mé & Chaillat, 1999). C-SET has been recognized as the official standard by the European Commission. This illustrates the fact that private networks, when they work closely with public authorities (national and regional), can become *de facto* regulators, or at least co-regulators. It might take the form of conceptualizing and promoting a solution, then asking for public authorization, at least administrative, but also legislative. Or it might take the form of a co-construction of techno-political regulation in close cooperation with public bodies.

The emergence of transnational regulation evolves in parallel with national specificities. Transnational regulation efforts must take into account local payment cultures, Internet usage rate, and the advancement of Internet connectivity infrastructures. Regulators, public and private, must find compromises, either by "transporting" a national model (considered by regulators-translators as a best practice), or by finding a lowest cost denominator (Pistor, 2000). The process of standardizing the law can provide ideas for regulators in the cyber payments' arena. The choice of a particular national legal order may reduce the costs of adaptation, as at least one country already complies with the new standards. However, at least if adopted by states, this approach smells of domination or "legal imperialism" (Pistor, 2000). Political reasons therefore make it unlikely that this approach is taken openly. Political factors should be taken seriously, not only because they may delay or dwarf the standardization effort, but because they will have a strong impact on reception of the standardized rule. Another method is the lowest cost denominator (LCD). This approach is frequently used for standardizing the law. It avoids some of the problems of choosing a particular legal order, because, at least in theory, the LCD should be compatible with pre-existing concepts and rules. However, this approach limits the scope of standardization. The minimum standards that are established do not preclude diversity in different jurisdictions. A compromise between the two approaches is to create a new legal concept based on comparative research and

to incorporate it into the standardized rule. This approach is appealing, because it avoids, or at least, mitigates some of the political problems of using a particular national legal order.

These approaches can be useful for cyber payments' regulators, by analogy. The difficulty resides in the synchronization of technical regulation and legal regulation. Let us look at the major payment issues under this perspective. There are two main topics: the regulation of issuing electronic money and the regulation of digital signatures. The main trend in the regulation of issuing electronic money in all countries is that only banks should be allowed to do so. This is in line with the position of the European Central Bank (ECB) and the EU Commission. But there are still some differences among countries. Mainly those countries with an early introduction of electronic purses, issued by non-banks (Denmark and Finland) wish to retain this regulation. But besides this, they all agree that more or less strong surveillance measures are essential. But it is also true that in all countries, you can find spokesmen who argue for more competition in the field of payment systems and more chances for non-banks too (Bohle & Riehm, 1999). These positions are mainly occupied by technology providers and merchants. But it is our impression that they are having no great impact on ongoing policy.

Looking at the field of digital signatures, two countries have passed special laws: Italy and Germany. In Denmark, first attempts to establish strong digital signatures (with recognition similar to that given conventional signatures) were stopped and a new moderate approach was developed. In Spain, there is no regulation at this moment concerning digital signatures, but the EU proposal (15.5.1998, KOM (1998/297)) has already stimulated preliminary activities such as the establishment of Fundacion para el Estudio de la Seguridad de la Telecomunicaciones (FESTE, Foundation for the Study of Security in Telecommunications).

The Issue of Banks Versus Non-banks

The issue of banks versus non-banks is thought-provoking. It operates as if would be regulators concentrated their effort in "kidnapping" the relation with public authorities to control the evolution of the regulators' club. Regulation is needed to add value to the consumer, but also to ensure political dominance of existing actors. The emergence of new actors is a real threat to banks. The challenge is to legitimate the network within certain limits and to align and police the stakeholders.

A few propositions could be presented. With regard to electronic payment systems, people expect that all payment systems should be interoperable within the EU: The multitude of access products as well as new e-money products are expected to be interoperable. In the end, the question of interoperability of payment instruments is less a matter of e-commerce, but a political and psychological task of fulfilling these expectations and avoiding frustration. It is not by chance that Commissionner Van Miert has investigated the high commissions taken for cross-border payments by banking institutions.

This is the reason why a common security infrastructure and a common payment infrastructure are needed (Bohle & Riehm, 1999). It is in this area that the experts are asking for regulation and responsible policies. With regard to access products, SET is not to be seen as a special payment standard, but as an element of a secure payment infrastructure. It is generally agreed that politics should not try to impose standards. Standards are understood as a result instead of as something to be set from the start. Standards usually result from bargaining between different interest and technical solutions (this is the very definition of translation in Latour's terms). Regulators may take the role of stimulator, catalyst, or moderator of standardization processes, but should refrain from public intervention. They should facilitate the emergence of acceptable standards as results of

negotiations-translations. Banks and bankcard networks act as translators of requirements. They propose and discuss solutions, which can become a regulation under public authorities' facilitation. European Parliament consults, the European Commission poses, and national parliaments appropriately adjust the European standard.

Interpretation of the SET Case Through the Translation Theory

Czarniawska and Sevon (1996) have shown that the term of translation (Callon, 1986) calls attention to a richness of meanings associated: transference, linguistic translation, but also transformation, alteration, and change. The term of translation is also associated with a constructionist view of power. For Callon and Latour (1981), "power" stands for a range of associations: actors associate with other actors (including non-humans), and the more numerous and important their associations are, the greater is the power of the whole network thus created. In this sense, power is a result but not a cause, and it does not "belong" to anybody in particular (Czarniawska & Sevon, 1996).

The construction of the SET norm can be analyzed as an illustration of the management of a controversy to help move toward a network reinforcement process. The controversy deals with security. The evolution of fraud on the Internet has caused a breakdown of the trust chain. Therefore, translators (bankcard networks, in this instance) endorse the role of putting together business requirements and "selling" them to the community, not as a package, but as a process, a process of negotiation, the confrontation of actors' interests materialized by a business requirements edited document (Sahlin-Andersson, 1996), and a physical prototype: a smart card reader connected to a personal computer (PC). Multiple intermediaries (Callon, 1986) intervene in the process (documents, actors, and data). They are used as factors and impediments of consensus building.

The standardization process goes through a phase of testing. Although often strictly technical, this phase can help build legitimacy for the tested solution. For example, in Australia, four major banks have chosen to participate in the testing of a secured e-commerce solution. Why have they chosen one partner instead of another? They have invested time, energy, and money with the organization with a capability and competencies to supply with the tools to implement the SET program. Implementation is a key element. It is as if translation's teleology was to facilitate implementation by the actors beyond the borders of the experimentation.

Translation means that there is freedom to conceive the solution (and its appropriate regulation package embedded into it). It is not given or imposed. Translation also means that the process of manipulating requirements and solutions goes through a step of search for equivalence between texts, statements in different contexts (Callon, 1986): a market demand in Sweden, to be translated by the London office of a bankcard network into software functionality by the computer scientists at the world headquarters in the USA.

Legitimacy is an attribute of the organization, related to its ability to build trust among partners. A bankcard network, composed of thousands of banks in more than 100 countries, brings legitimacy every time it undertakes an experiment. It starts the virtuous circle of translation. Organizational legitimacy encourages banks to become participants in pilot projects. Their participation improves the likeliness of success of such a project, which can pave the way to the development of a *de facto* standard.

The trust chain of human actors is a risk-reducing factor in the construction of regulation policy. In our example, the international network of bankcard members encourages the participation of Australian banks and provides them with a forum of discussion. These events act in favor of the SET 1.0 protocol. A good way of aligning actors is to expand the frontiers of a pilot to an entire industry, giving the experiment a real life dimension, thus improving the credibility and the readability of the results.

In France, CyberComm has taken the role, the posture of a SET translator. The power is a result of actors' associations, not a cause. It does not "belong" to anyone in particular (Czarniawska & Sevon, 1996). CyberComm has contextualized the French payment culture and problematized the security controversy, operated a formal investment (Boltanski & Thevenot, 1991), namely, the creation of a consortium, and instituted a compulsory crossing point for the payment card. It has taken a political stand, meaning that it has given the banks the opportunity to continue to govern the techno-political networks, even if telecommunications companies and technology providers become co-conceptors and implementers of payment solutions. The crossing point (PPO) acts just like a paradigm selection in the research process: It permits creativity, brings new interpretations, but, at the same time, it impedes creativity. PPO facilitates the conception of innovative solutions, but within the limits it has set.

The translator proposed a preferred way of handling the translation. There is only one translator for many actors, but there are "cascades" of translations, allowing each actor to become someone else's translator. SETCo. is a global translator, and a French banker can be the translator for his/her suppliers and customers. User education is a form of ultimate translation at the end of the trust chain.

Translation comes first as early as the conception phase of a project. Regulation comes next, in the implementation phase. But it might prove to be good governance to include regulation requirements in the conception phase, because choices will be irreversible after implementation.

Summary of the Interpretation Through the Actor Network Theory (ANT)

Let us look now at the steps of the translation process in our example:

First step: contextualization (actants, challenges, and move toward convergence): Professionals and customers demand Internet payment securization to facilitate electronic commerce development. Actants are banks, Internet merchants; one of the challenges is the development of SET; the convergence is in the common interest in developing a secured solution;

Second step: problematization and emergence of a translator: What unites the actants is the need for security at a reasonable cost (SET seems too costly to some experts); what separates public and private actants is the secret around encryption, and the entry of trust intermediaries (possibly non-banks);

Third step: compulsory crossing point (CCP) and convergence (it can be a location or a piece of text): The major bankcard networks act as CCPs in the collective search for convergence;

Fourth step: selection of spokespersons of each organization: CyberComm, networks, banks, governments, and consumerist associations select spokespersons;

Fifth step: formal investments: external (consortia, economic groups such as G.E.I.E.) and internal (regional committees, products' groups, coordination bodies, participation in normalization boards, etc.);

Sixth step: management of intermediaries (data, technical objects, money, know-how, etc.). In our example, the intermediaries can be reporting data, chip card, and card readers with their software, budget for Cyberpayments' R&D, or organizational learning capabilities in international risk management;

Seventh step: actors' mobilization (enrolment): alignment through the conception of systems integration and interoperability projects;

Eighth step: the search of network irreversibility: the creation of a European consortium, for example.

In summary, translation is an open and constructionist social process which crosses national borders and has significant impacts on law and public policies (law enforcement, money laundering, consumer protection,

etc.). One of the major trends of such a process is the search for common good's construction. There is a conceptual proximity with global information issues (in the GII project for instance).

If an analogy with Internet payment mechanisms is drawn, the authors can propose that regulation is needed in the interest of the consumer. But who will be the consumer's spokesperson? Who will propose a translation of his/her interests? And how? The authors have attempted to show an illustration of how it could work. The authors do not consider it as a best practice, but more as an example of one possibility of management practice to be articulated with transnational regulation policy.

Conclusions

The purpose of this article was to present and interpret the case study of the SET scheme of Internet security, as an illustration of the necessary construction of interoperability solutions for financial services. The interpretation of case data with ANT provides an illustration of power coalitions among banks to create a *de facto* standard for transnational electronic payment security on the Internet. Financial institutions in general and banks more specifically must be ready to accept alliances in order to develop secured and efficient instruments for international electronic transactions. This has proven compatible with inter-bank competition. The second challenge deals with non-banks. In a Web 2.0 society, they have the potential to act as substitutes of banking services. That is the reason why it is fundamental for banks to take the initiative in online banking and in the creation of new types of money, such as mobile money. This is not only a heavy investment but also a change in mentalities and a tension on corporate distinctive capabilities. Further research is needed to provide a decision framework for banks to follow.

References

Bohle, K., & Riehm, U. (1999). *Electronic payment systems in European countries.* Second draft, Forschungszentrum Karlsruhe.

Boltanski, L., & Thevenot, L. (1991). *De la justification (The justification)*. Paris: Métaillé.

Callon, M. (1986). Eléments pour une sociologie de la traduction (Elements for sociology of translation). *L'Année Sociologique, 36*, 169-208.

Callon, M., & Latour, B. (1981). Unscrewing the big Leviathan: How actors macro-structure reality and how sociologists help them to do so. In K. Knorr-Cetina, & A. Cicourel (Eds.), *Advances in social theory and methodology* (pp. 277-303). London: Routledge and Kegan Paul.

Campbell, A., & Verbeke, A. (1994). The globalisation of service multinationals. *Long Range Planning, 27*(2), 95-102.

Claveau, N., Martinet, A. C., & Tannery, F. (1998). Formes et ingéniérie du changement stratégique (Forms of engineering and strategic change). *Revue Française de Gestion (French Academy of Management), 120*, 70-87.

Collin, P. M. (2006). *Bâtir un Réseau Mondial de Services* (*Building a global network services*). Paris: L'Harmattan.

Czarniawska, B., & Sevon, G. (1996). *Translating organizational change*. Berlin: De Gruyter.

Dvořák, P. (2005). *Komerční bankovnictví pro bankéře a klienty (Commercial banking for bankers and clients)* (3rd ed.). Prague: Linde.

Folger, R., & Turillo, C. (1999). Theorizing as the thickness of thin abstraction. *Academy of Management Review, 24*(4), 742-758.

Gadrey, J. (1994). Les relations de service dans le secteur marchand (Service relationships in the market sector). In J. de Bandt, & J. Gadrey (Eds.), *Relations de services, marches de services (Relations services, marches services)* (pp. 23-41). CNRS.

Haguet, J. (1996). *L'Internet: Guide stratégique pour l'entreprise (The internet: A strategic guide for business)*. Paris: Masson.

Hirst, P., & Thompson, G. (1996). *Globalization in question*. Cambridge: Polity.

Latour, B. (1989). *La science en action (Science in action)*. Paris: La Découverte.

Leyshon, A., & Thrift, N. (1997). *Money/space: Geographies of monetary transformation* (pp. 225-259). London: Routledge.

Machková, H. (2009). *Mezinárodní marketing*. Prague: Oeconomica Publishing.

Mé, L., & Chaillat, R. (1999). Le commerce électronique: Un état de l'art (Electronic commerce: A state of the art). *An Overview of Electronic Commerce* (Unpublished document, Supelec School, Paris).

Newman, D. (1998). Boundaries, territory, and post-modernism: Towards shared or separate spaces. *Geopolitics.*

Ohmae, K. (1995). *The end of the nation state.* New York, NY: Free Press.

Pistor, K. (2000). The standardization of law and its effect on developing economies (pp. 6-8). *United Conference on Trade and Development*, G-24 Discussion Paper Series, Harvard University, Center for International Development.

Porter, M. (1991). Towards a dynamic theory of strategy. *Strategic Management Journal, 12*(S2), 95-117.

Reidenberg, J. (1996). Governing networks and rule-making in cyberspace. Information Security Committee.

Sahlin-Andersson, K. (1996). Imitating by editing success: The construction of organization fields. In B. Czarniawska, & G. Sevon (Eds.), *Translating organizational change* (p. 82). Berlin: Walter de Gruyter.

Taušer, J. (2007). *Měnový kurz v mezinárodním podnikání (The exchange rate in international business)* (p. 162). Prague: Oeconomica Publishing.

Toal, G. (1999). Borderless worlds? Problematizing discourses of deterritorialization. *Geopolitics, 4*(2), 139-154. In N. Kliot, & D. Newman (Eds.), *Geopolitics at the end of the twentieth century: The changing world political map*. London: Frank Cass.

Tsoukas, H. (1996). The firm as a distributed knowledge system: A constructionist approach. *Strategic Management Journal, 17*, 11-25.

Virilio, P., & Lotringer, S. (1983). *Pure war*. New York, NY: Semiotext.