Electronic Markets and Security Requirements - The Legal Basis

Security and the legal recognition of new techniques such as electronic signatures will be crucial factors for the realization of electronic markets. Caused by the privatization of telecom services, the responsibility to take security measures is often ambiguous and has to be clearly defined between the contractual parties.

** by Dr. Bruno Wildhaber*
R^3 Security Engineering AG

Electronic markets and EDI are becoming more and more popular. Although the technical features are widely known, there is still a notable general and juridical uncertainty about the liability and the responsibilities of the parties involved. This paper concentrates on the legal situation in Switzerland. However, the security aspects will also be valid from the international point of view. Especially in a crossborder situation, where there are no more physical borders and where data flows freely, security measures cannot target on an isolated and clearly defined environment anymore. In IS security, controls are more than just technical and organizational measures to secure availability, integrity and confidentiality. *Control encompasses the policies, procedures, practices and organizational structures that assure the adequacy of information asset management and the consistency and reliability of IS activities.* The integration of classic EDP techniques with telecommunications (telematics) increases the demand for controls, where more than just technical aspects are considered. This paper will treat the legal framework and the associated technical questions.

Legal Framework

Most of the recent developments of information interchange, like electronic signatures and EDI, are not yet represented in most of the European laws. A stable legal framework under public law has to be established to assure a trusted legal environment. In the meantime, there will be an urgent need for well defined contractual relations. The private agreements are limited, they can only be legally binding for the contracting party, thus automatically limiting the chances of open markets in todays legal framework. The simplified situation in figure 1 is showing the typical relations between public and private law: Although there are countries like Germany where the relations between the PTT are nowadays stipulated under private law, most of the key points, like the liability rules, are still based on public law and there is only narrow margin for private arrangements. Some laws are already directly affecting electronic dataflow and related security measures. In Switzerland, there are mainly two laws which have to be taken in consideration:

- 'Fernmeldegesetz', October 1991 (Telecom Law, FMG; and statutory order, VFMG),
- 'Datenschutzgesetz', July 1993 (Data Privacy Law, DSG).

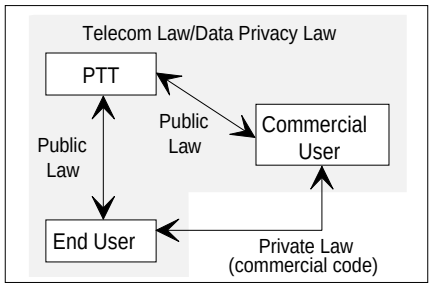

Figure 1: Legal Framework

Telecom Law

Based on the old postal law, the telecom law extends the old *secrecy of letters* (Postgeheimnis) to the *secrecy of telecommunications* (Fernmeldegeheimnis, Art. 15 FMG). This is a peremptory rule and has to be applied to everybody who is offering telecom services, and applies also to the suppliers of enhanced services. It is therefore illegal to reveal any details about the contents, the parties and all other data in factual relation to the offered service. The supplier is even obliged to take all necessary care that the secrecy of telecommunications will not be compromised by any other party. There is no immediate indication in the law as to which measures have to be taken. There are some indications, however, which allow the quality and quantity of security measures to be defined.

Service Structure

Services are split up into the so-called 'Grunddienste' (Basic Services, Art. 3 lit. f FMG) and 'Erweiterte Dienste' (Enhanced Services, Art. 3 lit. g FMG). Any processing of information which is more than normal transmission will be considered as enhanced service (Art. 3 FMG). This separation of services is of main importance to the commercial user, due to the fact that the basic services will be reserved for the Swiss PTT only. However, the PTT also holds the postal privilege on the so-called 'Teledienste', e.g. telephone, telegram and fax.

Data Privacy Law (DSG)

According to Art. 7 DSG personal data has to be protected by the use of appropriate and proportional security measures. A more detailed description can be found in Art. 9 VDSG. The responsibility lies with the data owner. In cases, where personal data will be processed outside the owners facilities, e.g. transmitting and storing data, the owner has to make sure that the mandatory will treat the data the same way he is allowed to (Art. 11 DSG). The supplier of enhanced services who is processing personal data is subject to the Privacy law, which means that he might be obliged to notify his data processing activities (Art. 11 DSG).

Security measures

According to the described service split, the PTT takes measures concerning OSI layers 1-3, primarly physical security over a point to point connection with error correction and controls of logical channels (ISO 7498-2, 8072 and 8073). ISO 7498-2 defines so called 'security services', including confidentiality, data integrity, access control, authentication, and non-repudiation. Suppliers of enhanced services use OSI-layers 4-7 and will have to control the access to their application systems, granting confidentiality and data integrity and assure non-repudiation. Some controls or 'security services' cannot be clearly assigned to a certain layer. Due to the fact that many of the really important controls are to be found in either layer 3 or 4, it has to be defined by the parties who will be responsible for processes like authentication or encryption. Otherwise the situation may arise that due to a lack of control a security breach will be created. Therefore, all suppliers of enhanced services should inform themselves about the security measures taken by the PTT to be able to judge on their own which additional security measures will be necessary. There might be a solution available by using the OSI 'security frameworks', describing the concepts of each service. This can help to sort out tasks, but for each individual case a risk analysis should be performed and the security measures and responsibilities ought to be stipulated.

Liability

The liability of the PTT for undeliberate action or normal negligence has been limited to 1 million Swiss francs according to Art. 47 FMG and Art. 82 FDV. There will be no limitation for deliberate action or gross negligence. Liability for private suppliers is not limited, but contractual limitations of liability can and must be established. The necessary measures will be judged according to the state of the art and to their proportionality.

Conclusions and Problems

The legal framework seems to be clear, all parties in an electronic market will have to establish state-of-the-art security measures. But there are still many open questions about the ways of how these measures have to be implemented. As soon as processing of personal data takes place, the data privacy law has to be taken into consideration. In order to achieve a secure environment, the security framework has to be discussed between the PTT and all other parties. ■

References

[1] *Borner, S. et al.:* Das neue Fernmeldegesetz: Europäisches Kleid oder Schweizer Korsett?, Chur/Zürich 1991, pp 83-85.

[2] *Cooper, J.A.:* Computer & Communications Security, Strategies for the 1990s, New York 1989.

[3] *Dykman, C.A. (Ed.):* Control Objectives, Controls in a Computer Environment: Objectives, Guidelines and Audit Procedures, 4.ed., Carol Stream (USA) 1992.

[4] *Fumy, W.:* Sicherheitsstandards für offene Systeme, Datenschutz und Datensicherung 6/1991, pp 288-295.

[5] *Wildhaber, B.:* Informationssicherheit, Rechtliche Grundlagen und Anforderungen an die Praxis, Zürich 1993, pp 53-57.

Dr. Bruno Wildhaber is a senior consultant with R³ Security Engineering, Aathal, Switzerland. He is a member of the board of the EDPAA (ISACA) Switzerland Chapter.

Research Issues

Process Authority Redesign and Electronic Markets

European businesses today are showing a significant interest in the concept of business process redesign, not in the least because its advocates promise a dramatic decrease in costs and a similar increase in sales. Since information and communication technology seem to play enabling roles, one can expect electronic markets to be significantly contributing to the effects of business process redesign.

** by Hans van der Heijden, Prof. Dr. Jo van Nunen and Prof. Dr. René W. Wagenaar Erasmus University*

Formulated in a simple way, process redesign encompasses the radical redesign of organisational processes in order to increase efficiency and/or effectiveness dramatically. Information and communication technology are being viewed as necessary enablers [1] [2]. Basically, the idea is to review the organisational processes, the organisational participants and the organisational information systems in such an innovative way that a maximum increase in effectiveness is gained. However, many redesigns fail, primarily because of their radical nature [2]. Radical changes in an organisational design imply major organisational changes, that, above all, require careful preparation, the commitment of top management, and the willingness to change by all relevant members of the organisation. The change part is often isolated from the process redesign research area and termed process implementation [1].

Process Redesign

Process redesign and process implementation together have been called process innovation [1] and process re-engineering [2]. If we focuss on the process redesign area, we see that typical questions of practitioners are: "What should a process redesign look like?" and "How can I measure benefits a priori, in order to balance the new designs against their costs of implementation?". In order to answer these questions, academic researchers find themselves confronted with questions such as "In what way can we generalise over particular process redesign examples, i.e. what particular dependent and independent variables seem to be involved and how do they interrelate?" and consequently, "What modelling techniques are suitable to evaluate changes in those variables and to quantify and qualify results?". At the Rotterdam School of Management we have begun to address these questions, for example with the development of two tools: the decision support system Edialysis, which provides managers insight in quantifiable costs and benefits of Electronic Data Interchange (EDI) and the management game Port of Rotterdam, which provides managers with insight on the qualitative, long term effects of EDI.

Classes of Redesign

There are several organisational research variables relevant to business process redesign:

- In the first place, the *sequence* of the processes can be changed. By decoupling processes which depend on each other, sequential processes can be carried out partly in parallel. Similarly, processes that do not directly depend on each other can be coupled at later stages. A famous example of sequence redesign, implemented at a large American car company, is releasing payment without invoice [2]. Rather than waiting for the invoice, the company decided to pay when the goods had arrived. Information technology was used to compare and prepare the necessary documents.
- In the second place, the *location* of the decision processes may change. Communication technology strips the word 'distance' from most managerial decision making. Processes are no longer hooked to particular locations, because data or knowledge can be made readily accessible at almost any site. This can eliminate, for example, the need for regional offices, since field personel, equipped with proper communication technology, can be allowed to process data directly to and from the head office.
- In the third place, the process *authorities* can be changed. By using information and communication technology, organisational members can be authorised to perform or govern a broader range of processes. Of course, all three major classes of redesign, sequence, distance and authority, may require subprocesses to be added, deleted, or modified.

Electronic Markets

We would like to focus on process authority redesign and the role of electronic markets therein. Electronic markets can be defined as information systems that input bids and offers submitted by buyers and sellers and output trades for which those bids and offers have been matched [3]. Electronic markets can be found in industries such as tourism, insurance, finance and transport. In transport, electronic market systems frequently pay significant attention to the logistical side of the transaction, for example by allowing the user of the electronic market to coordinate and control the entire transport process from shipper to consignee. The rise of such advanced control systems puts the existing industry structures in transport under pressure: a major question here is whether the authorities to arrange transport will shift due to these advanced options - eg. from a shipper to a forwarding agency, from a forwarding agency to a consignee, etc.