2 TECHNICAL ENFORCEMENT OF INFORMATIONAL ASSURANCES

Joachim Biskup

Abstract: Dealing with informational assurances we have to consider the full complexity of the information society. In a narrower sense informational assurances comprise informational rights, the related legal and social rules as well as the enforcing technical mechanisms. The right of privacy, understood as informational self-determination, is taken as an important example. Starting from a discussion of present shortcomings in technically enforcing this right, we outline some recent developments in the German and European legislation concerning privacy, teleservices and digital signatures. Also some selected mechanisms for improving the technical enforcement are evaluated, including federated system structure and local security autonomy, cryptographic protocols enabling cooperation under threats, and the tamper resistant hardware foundation. Finally, we advocate the shift from the traditional paradigm of reference books implemented as centralized databases to the new paradigm of communicating personal data agents. The new paradigm is devised to enhance the data subject's means to technically enforce the interests concerning privacy.

2.1 INTRODUCTION

Over the last decades the vision of what is called the "information society" has evolved. Some features of this vision have already become reality, others are still nebulous and open for the future. Both sides, the technical innovations in the past and the further developments in the future, challenge our communities: the past technical achievements strongly require new and adapted social foundations, and the ongoing technical projects demand a careful social design. Democratic societies already started to become aware of these challenges and partially responded to them. Two mainstreams of activities can be identified,

S. Jajodia (ed.), *Database Security XII*

privacy protection and evaluation criteria for critical computing systems. Each stream has its own weaknesses, and even both streams together cannot cope with all issues.

2.1.1 *Privacy protection*

The first sort of activities concerns individual privacy. Here fundamental human rights of individuals are sought to be protected against the assumed overwhelming informational power of public institutions and private companies. The basic legislation decrees so-called "informational self-determination", i.e., in principle, each individual citizen can freely decide on whom he gives what part of his data and on what kind of processing his data he is willing to agree. According to this principle, an individual should retain full control over processing and disseminating his data. However, this principle is questioned by *conflicting social goals*, *technical difficulties* and the *lack of* effective and efficient *technical enforcement mechanisms.*

Examples of *conflicting social goals* are public security, law enforcement, national defence, social and health services, scientific research, freedom of press, participation in public decision, or trade interests. Basically, legislators dealt with such conflicts in two ways: the basic privacy law simply declares that some agencies or institutions are exempted from the principle, or the basic law refers to additional, so-called sector-specific laws each of which regulates the conflicts for some restricted domain. Critics, however, argue that there are too many global exemptions and that sector-specific laws do not cover all relevant domains and lack coherence.

Technical difficulties mainly group around the following four observations. 1. Once an individual has disclosed some of his data (understood as knowledge about him), deliberately or under legal compulsion, this data (understood as some digits) is processed within a computing system that is under the control of someone else. While, ideally, a subject is entitled to control his data (knowledge), this data (digits) is not physically available to him but just only to those agents against whom, among others, his privacy should be protected. 2. The correlation between data as knowledge and its encoding as digits is inherently difficult to monitor. In some cases it is even deliberately blurred, for instance by a cryptographic encipherment. 3. Digital data can be easily duplicated and may be spurious. 4. Much data (as knowledge) is not merely personal but deals with social relationships with other individuals within the real world, for instance data about matrimonial or childhood status or about medical treatments. Accordingly, also within the computing system this data (as digits) is not unambiguously connected to a personal file but may be spread across the files of all the persons involved, or the data even disguises as pointers or related technical concepts.

Legislators appear to have dealt with the first three technical difficulties only rather weakly. Basically, the first observation is treated by penalties and some supervision, the second one by a somehow sophisticated though not technically elaborated definition of "personal data" (as any information relating

to an identified or identifiable natural person), and the third one by a technical appendix to the basic privacy law which states some high-level, declarative rules of well-controlled data processing.

The fourth observation on the relationships seems to be completely ignored, and in fact it may also be seen as already resulting from another kind of conflicting social interests. Whereas the conflicts mentioned above are between a weak individual and a powerful institution, the conflicts inherent in social relationships may also arise between individuals of equal strength. Moreover, even without any conflicting interests, the problem of how to represent real world relationships within the formalism of a computing system has been intensively studied in the field of data modelling but not generally been solved.

The *lack of technical enforcement mechanisms* for the principle of privacy is mainly due to the problems already discussed before: without a socially agreed settlement of conflicts we cannot construct fair technical enforcement mechanism; the postulated ideal control and the actual physical control are separated; the semantics of digitally stored data with respect to the outside world are rarely captured algorithmically; and the physical possibilities of manipulating and duplicating digital data cannot be fully controlled using only traditional data processing techniques but would strongly require to employ new technologies like cryptography.

2.1.2 Evaluation criteria and computing security agencies

The second sort of activities responding to the challenges to the information society is directed to assist organizations in running their computing systems in a secure way. Here the organizational needs and interests are sought to be protected against accidental or malicious misbehaviour of people, or of system components devised by them. In contrast to the activities on privacy protection there is no general legislation, but the states founded specialized new computing security agencies, which, at least at the beginning, happened to be closely related to previous or existing security agencies. The computing security agencies are supposed to publish evaluation criteria for secure computing systems (see for instance [55, 17, 16, 18]), to evaluate products against these criteria (or to supervise other institutions carrying out such evaluations), and to give advice to organizations of public interest concerning security in computing systems.

In the early stages military needs and their interest in strict confidentiality (against the assumed enemy) dominated. Accordingly, early evaluation criteria were strongly influenced by the Bell-LaPadula model of restricting and controlling the data flow within a computing system. But already then, not only confidentiality but also availability of data and other computing resources as well as their integrity have been recognized as important security goals. All goals, however, were mainly treated from the perspective of a centralized, strictly hierarchical organization running centralized computers for a specific unquestioned purpose.

As time went by, both the scope of the evaluation criteria broadened and computing technologies changed dramatically. In the public and commercial

sector integrity and availability were preferred to confidentiality, and computer networks and workstations suffer from vulnerabilities and offer options which differ from those of traditional mainframes. The computing security agencies have reacted with and still work on a series of amended evaluation criteria, the latest are the so-called Common Criteria.

The Common Criteria [18] can be characterized by two important features. Firstly, they take into account the international flavour of the "information society", i.e. its participants live in a globalized informational environment and thus the security of their computing systems have to be evaluated according to a broad international perspective. And secondly, within that globalized environment there are many different needs and interests around, i.e. the various participants should be supported to define their specific protection profiles and security targets.

Although many shortcomings of the restricted purely military oriented point of view on centralized computing systems have been eliminated, the Common Criteria still do not adequately face the large variety of today's computing systems, and they do not appropriately cover the evolving reality of everyone's computing environment with publicly available international telecommunication, Internet, personal computers and digital service providers.

2.1.3 Unsolved issues

Roughly speaking, the weaknesses of both streams of activities can be summarized as follows.

- The privacy-oriented stream deals with the legal issue of fundamental rights of individuals, but it does not seriously consider to balance all other rights involved, and it does not thoroughly take care of the technical enforcement of its requirements.
- And the evaluation-criteria-oriented stream emphasizes technical enforcement of security but it largely ignores social and legal issues within a democratic society.

Even worse, though the technical guidelines of evaluation criteria can also be helpful to operating computing systems which manage personal data, they are not at all tailored according to the technical enforcement of privacy.

In order to respond to the challenges of the evolving information society, we need a much broader approach: A *political discussion* aiming at a balanced social solution of and a coherent legislation on all aspects of digitally processing information and of digitally delivering services. And a *scientific development* aiming at the actual technical enforcement of the social and legal rules we will have agreed upon.

In particular, the political discussion has to consider all parties involved and their possibly mutual conflicting rights and interests, and it has to be consistent with the actual and future state of technologies. And science has to elaborate on all sensible social options in order to provide suggestions for their effective and efficient technical implementation.

The rest of this paper is devoted to direct the reader's attention to some recent contributions towards these goals. It is not intended to present a complete survey (that would be beyond the scope of the author's present resources) rather it concentrates on selected topics that the author believes to proceed in the right direction (and that the author is acquainted with from his actual experience).

2.2 INFORMATIONAL ASSURANCES

2.2.1 An outline of the information society

The "information society" comprises all individuals, participating in or being affected by electronic information processing, as well as their public institutions of any level and their private companies of any size. These individuals, institutions and companies are tied together by a historically achieved and further developing framework of informational and other rights and interests which, in some instances, might be shared or, in other circumstances, might be in conflict.

Seen from the perspective of this discussion, the information society is technologically based on public or private telecommunication services, on which computerized networks for all kinds of computers are run, for example ranging from personal computers over office workstations with local or specialized global servers to powerful mainframe computers. Such networks are used for a wide variety of purposes, in particular to exchange raw data, like email, to provide informational services of any kind, like daily news, video entertainment, event and transportation schedules or database records, and to support informational cooperation like home banking, electronic commerce or certifying digital documents.

Additionally, in response to the challenges mentioned above, the information society should be based on a coherent and balanced system of informational rights and socially agreed and legally founded rules as well as of mechanisms that support the participants in enforcing their issues. Such a system has been suggested to be called (in German) "informationelle Garantien" [31], and in the next subsection of this paper a further outline and elaboration will be presented under the keyword "informational assurances".

2.2.2 A framework of informational assurances

Dealing with informational assurances we have to consider the full complexity of the information society. In particular we have to uniformly cope with

- all its *participants* comprising both the individuals and the groups that are formed by them ranging from public institutions over civil associations to private companies,

- their informational *rights*,

- their specific *needs* and *wishes* for *information*, informational *services* and informational *cooperation*,
- their specific *interests* for such informational activities,
- the mutual *conflicts* among such rights or interests,
- the anticipated *threats* to such rights and interests,
- the necessary basis of *trust* that is required for fulfilling such needs and wishes,
- the social and legal *rules* for that trust,
- and the technical *mechanisms* that can enforce such social and legal rules as a matter of routine in daily live.

Informational assurances in a narrower sense comprise the informational rights, the social and legal rules as well as the enforcing technical mechanisms.

By the very nature of the information society, nearly *every* individual, institution, association or company has to be treated as a *participant*. A participant may play an active role, or he might be only passively affected by the actions of other participants. In general, every participant will be involved in many ways.

Informational *rights* always arise with a double meaning. On the one hand, a participant is entitled to behave how he is named here: he has all civil rights to *participate* in the activities of the information society and to take advantage of them. On the other hand, if being an individual, a participant enjoys the fundamental human rights, including privacy in the sense of informational self-determination, and also otherwise he is the object of all kinds of *protection* that a state offers: in any case informational activities should not be harmful to him. Therefore many informational activities should be both enabled and restricted by law and its enforcement.

Based on general informational rights on participation, a participant can actively pursue his specific informational needs and wishes. His demands may be concerned with a wide range of activities, which can be roughly classified as follows: *information* as such (meaning that he is providing or collecting and processing any kind of data that seems relevant to his participation), *informational services* (meaning, for example, that he is asking for or delivering press services, electronic entertainment, database retrieval, etc.), or *informational cooperation* (meaning that he is involved, for example, in some role of electronic commerce, electronic voting, document certification, etc.).

Once a participant is involved in some informational activity, actively or passively, he is following several *interests*, which may vary considerably depending on the specific situation. I advocate that the goals commonly cited for defining computer security, namely *availability*, *integrity*, *authenticity* possibly with *non-repudiation*, *confidentiality* and others, should be understood first of all as specific interests of participants within an informational activity.

Both the general rights, based upon which participants are involved in some informational activity, and the specific interests of the participants involved may turn out to be conflicting. Indeed, they will be in conflict most of the time. The *conflicts* arise from the different active roles and passive affectednesses in an informational activity.

Each conflict may result in *threats* to rights or interests. In fact, in case of conflicting issues, one participant following his issue appears as threatening the conflicting issues of another participant. Additionally, we are also faced with threats resulting from the accidental or malicious misbehaviour of some participant. Such a troublemaker may be intentionally involved in the informational activity, or he may come more or less from outside, for instance misusing some computing facilities that are available for him because of his general rights of participation.

Although there are in general unavoidable conflicts and threats, informational activities, seen as purposely arisen interaction of participants, must be somehow based on trust. Ideally, a participant would prefer to *trust* only those other participants that he can exercise some kind of control over. Practically, however, the case of having direct control over others rarely occurs. Basically, there are two ways of solving this dilemma.

In the first way the assistance of further participants is required. They are intended to act as some kind of notary or arbitrator, which are to be trusted by the original, possibly mutual distrusting participants. In the second way the trust is shifted to some technical equipment, more precisely to the people delivering that equipment.

For any kind of trust, we need some *social and legal rules.* They are required either to establish trust, as, for example, in a notary or in the Technical Control Board, or to deter misbehaviour, or, if this fails, to deal with the consequences of misbehaviour. Such rules have to be enforced somehow. For hopefully rare cases, this task is the role of law courts.

For the routine cases of daily life in the information society, however, it appears desirable to shift most of the enforcement burden directly to technical mechanisms. By the design and tamper resistant construction of such *technical enforcement mechanisms*, it should be just technically infeasible to violate the rules, or, otherwise, the mechanisms should effectively provide sufficient documented evidence against a violator.

2.2.3 The interrelationships of political and technical aspects

It is worthwhile to note how the *political aspects*, dealing on one side with informational rights and on the other side with the social and legal rules for trust, are intimately intertwined with *technical aspects*, concerning on the one side informational activities and on the other side technical mechanisms to enforce rules. As a full discussion of the interrelationships of these aspects is beyond the scope of this paper, we only state some short observations.

In most cases informational rights are based on traditional fundamental human and civil rights. These traditional rights are reinterpreted and concretized

with respect to the new technical possibilities of informational activities. Some of these new possibilities, however, may not be appropriately captured by the traditional rights at all. In that cases, the fundamental human and civil rights have to be augmented by additional, newly stated informational rights. For example, the right of informational self-determination has been directly derived from fundamental human rights of self-determination (in Germany stated as Article 2(1) in connection with Article 1(1) of the Constitution). But certifying public verification keys for digital signatures and using digital pseudonyms need to be treated by some newly created right (that has to fit traditional rights, of course).

Informational activities are not merely technical, but also or first of all, depending on the point of view, they constitute social interactions. As such they require some trust among the participants and, additionally or substitutionally, in their social environment. This trust in turn has to be founded in social and legal rules.

Social and legal rules for trust should have a technical basis for ensuring that they are routinely manageable for the massively occurring and more or less only technically observable informational activities. Thus they require technical enforcement mechanisms.

Surely, such technical enforcement mechanisms may affect informational rights, and it may happen that they impact the originally wanted informational activities and the required social and legal rules.

Summarizing, we can see a feedback loop where political aspects are followed by technical aspects and vice versa. Each of these aspects occurs on two levels: on a high and more or less declarative level (informational rights, and informational activities, respectively), and on a lower and more or less implementational level (social and legal rules, and technical enforcement mechanisms, respectively). Of course, a closer inspection would show more detailed levels and additional feedbacks.

2.2.4 The health care example

The field of health care provides good examples of both the interactions of the various aspects and many subtle details. Here we can only shortly sketch some points. A comprehensive study [51] has been performed, for instance, by the SEISMED consortium within the Advanced Informatics in Medicine program of the European Union. Some more personal views on this topic are contained in [7, 8].

Everybody is supposed to share the fundamental right to take advantage of medical services. This right is complemented by the health care professionals' fundamental legal obligation to provide their services at their best. And there are important additional social and legal rules involved, for instance for professional secrecy, control on epidemics, freedom of medical research, cost effectiveness, or for health insurances. With the emergence of computer and telecommunication technologies an important part of health care procedures can now be considered as informational activities where nearly everybody is

involved in various active roles and passive affectednesses, not seldom even simultaneously. Thus, the fundamental rights of health care as well as the additional rules have to be adapted to the new situation in order to ensure that appropriate information technologies are selected and dependably operated in an agreed mode.

Since, whether following a conscious decision or just as a matter of fact, the information technologies involved tend to be open federated systems of more or less autonomously participating components, the technical basis for the adapted rights and rules should be incorporated in the components themselves, as far as possible at all. Thus we are faced with the challenge to provide technical enforcement mechanisms that are located in the federal components and are under the physical control of their owners, i.e. of the human interest holders. Apparently, cryptography that is based on personal tamper resistant hardware devices and trustworthy certification procedures appears to be indispensable. But also the collection and maintenance of personal data should be reconsidered in order to substitute today's centralized data repositories by networks of communicating personal data agents whenever the social or legal rules ask for personal control exercised by the affected data subjects.

In fact, I strongly argue that we can comply with strong versions of many rules only by combining cryptography with personal data agents. Certainly, if this vision was realized, in turn we would need new rules for the anticipated personal computing, in particular for ensuring the availability of data that is socially or contractually required. This need would arise because the first technical problem with respect to privacy protection, as stated in Section 2.1.1, would be converted into its symmetric counterpart. Whereas now a data subject is concerned about some other participant having actual control on his data, in the vision that other participant would worry to get the subject's data actually transmitted when required at some point of time.

2.2.5 The situation in Germany

In Germany, legislation on privacy started with the "Bundesdatenschutzgesetz" (Data Protection Act) [14] which was declared in 1977 and essentially amended in 1990. The amendment was based on a sentence [15] of the Bundesverfassungsgericht (German Constitutional Court), which postulated the informational self-determination as part of the fundamental human rights. Accordingly, the law specifies that the processing of personal data is admissible only if at least one of the following conditions is met: the affected person has willingly agreed on the processing or that law or some other legal regulation allows it. There are some sector-specific legal regulations, in particular the so-called "Sozialgesetzbuch", which covers processing of personal data within the system of social security and health care. The underlying idea is to balance the fundamental right of informational self-determination with the practical needs of efficient and cost-effective daily life procedures.

While legislation on privacy has exhibited the tendency to be protective, i.e. to restrict the data processing, which has already evolved anyway in the past,

recent legislation on teleservices and digital signatures [25] is more directed to enable future good practice.

The Teledienstegesetz (Teleservices Act), as Article 1 of the Informations- und Kommunikationsdienste-Gesetz (Information and Communication Services Act) [25], aims at establishing "uniform economic conditions for the various applications of information and communication services", like for example telebanking, Internet access or electronic commerce. This law states that teleservices can be freely offered, subject that the service complies with general legal rules, and it limits the service providers' responsibility for the information content on their own part, thereby mostly excluding responsibility for mediated parts.

The Teledienstegesetz is complemented by a sector-specific data protection law, the Teledienstedatenschutzgesetz (Teleservices Data Protection Act), as Article 2 of the Informations- und Kommunikationsdienste-Gesetz (Information and Communication Services Act) [25]. Among other features, it obliges service providers to offer clients using the services anonymously or under pseudonyms. Thus, besides the traditional aspect of privacy concerning the confidentiality of personal data and its actual protection, the law takes care of a second aspect of privacy, namely of non-observability of personal behaviour. However, presumably the relevant obligations, as stated in the law, will be rather weak in practice, because anonymity and pseudonyms are required only under the proviso that these features are "technically feasible" and that they can be reasonably expected.

The Signaturgesetz (Digital Signature Act), as Article 3 of the Informations- und Kommunikationsdienste-Gesetz (Information and Communication Services Act) [25], mostly deals with a legal and organizational framework for establishing trust in using digital signatures. In particular, it defines rules for licensing certification authorities and for their procedures to provide evidence for a relationship between some natural or juristic person and a public verification key for digital signatures. It obliges the certification authority to reliably identify that person that may demand to get certificates under a pseudonym. Interestingly, the law also contains an article on "technical components". Its intention is, basically, that the purpose of digital signatures is actually met by the computing systems run by the certification authority. Therefore it requires that the technical components are sufficiently tested according to the state of technology and are approved by some institute acting on behalf of the licensing authority.

The Signaturgesetz is complemented by a so-called Signaturverordnung (Digital Signature Ordinance), SigV, [24] which among others details the requirements of the law pertaining the technical components. These requirements state all the nice features that you expect for digital signatures related to key generation, storage of a secret signature key and controlling access to it, adequate determination of data to be signed, secure register of certificates, and correct time-stamps. The ordinance also tells how to get assured about such properties, namely on the one side by a catalogue of suitable security measures

to be published in the Federal Gazette, and one the other side by an evaluation according to the evaluation criteria, as discussed in Section 2.1.2.

It must be emphasized that the law is expected to be widespread applied in both the public and commercial sector, and thus to substantially enhance future informational cooperation, but literally it is only some kind of proposition to the participants of the "information society", and it does not exclude any other means to make their cooperation trustworthy. Thus only future practice will finally show how the participants will behave and how courts will decide on disputes.

It should be clear from the preceding paragraphs that the sketched approach to dealing with legally binding electronic statements are an important step towards complying with a framework of informational assurances, as presented in Section 2.2.2. In particular, the subtle interrelationships between political and technical aspect are dealt with by connecting the legal rules directly to technical enforcement mechanisms. Thus in this field we can see a promising attempt to address the unsolved issues, identified in Section 2.1.3 with respect to privacy and technical enforcement.

The German computing security agency is called "Bundesamt für Sicherheit in der Informationstechnik" (Federal Agency for Security in Information Technology), BSI (cf. `http://www.bsi.de`). It was founded in 1990 as an authority in the portfolio of the Ministry of Interior. The surveillance tasks defined in the Digital Signature Act (and other tasks) are part of the duties of the "Regulierungsbehörde für Telekommunikation und Post" (Regulary Authority for the Telecommunications and Posts), RegTP, (cf. `http://www.regtp.de`) which was founded in 1998 in the portfolio of the Ministry of Economics as some kind of successor of the former Ministry of Posts.

2.2.6 The situation in Europe

The member states of the European Union (EU) have rather different traditions in dealing with data protection and related legal issues, see for instance [53, 36, 54], comprising, say, the German perspective of the individual's right of informational self-determination as well as the Swedish point of view that citizens must be able to control their local administration and thus should be allowed to inspect the files of the administration.

Originally founded as a community emphasizing a common and free market, the EU is recently evolving towards a political union as demonstrated by the agreement signed in Maastricht in 1992. Accordingly the EU now has to deal with the fundamental rights and needs of its citizens, too, and thus also with privacy, informational self-determination and related concepts. Furthermore, these rights and needs of individuals have to be balanced with conflicting goals, in particular with the original trade interests within Europe and with sovereign rights of the member states concerning national and public security.

As one of the results, the EU finally accepted a Directive on Data Protection [27] in 1995. Although announced to support a high level of protection, and being an important first step for Europe indeed, nevertheless the directive ap-

pears as a (too weak) compromise between the diverging pressures of national governments to maintain national law traditions and to exempt important areas of data processing from restrictions. See for instance [35, 54] for critical remarks.

After years of stagnation, as seen from the outside —or apparently more likely of confrontations, as seen from the inside— the European Commission recently came up with several documents [28, 29, 30] on informational services and cooperation, in particular with a communication on a "European Framework for Digital Signatures and Encryption", a communication on "The Need for Strengthened International Coordination", and a proposal for a "Directive on Digital Signatures". These documents emphasize the need of strong cryptography for supporting the citizens' requirements on acting within the information society, in particular with respect to authentication, integrity and confidentiality. Though we cannot expect yet that all national governments will finally fully agree to the Commission's points of view, there is presumably a high interest in declaring European mandatory directives as soon as possible. This expectation applies at least to the less controversial field of digital signature which are widely accepted to be crucial for electronic commerce. The field of encryption, though also identified as crucial for informational services and cooperation in general, may turn out not to be mature for a final European conclusion in the near future, unfortunately.

2.2.7 A notion of security

Within the framework of informational assurances, as sketched in Section 2.2.2, any formal notion of security for the technical enforcement mechanisms should be embedded in an overall reasoning about all relevant aspects and comply with the diversity of interests of the participants involved. The commonly used keywords for security —availability, integrity, authenticity possibly with non-repudiation, confidentiality and others— merely express such interests in a high level declarative way, and, accordingly, they have to be substantially refined for all of the participants' views on a specific informational activity. In the next paragraphs, the author's own approach [6, 7] towards defining an appropriate notion of security is shortly outlined; a more thorough discussion of this topic can be found, for instance, in [43]; a recent study to relate a broad perspective of security, so-called *multilateral security*, to evaluation criteria and certification can be found in [48, 49].

Basically, the approach follows the framework of informational assurances. The proposed formal notion of security results from capturing the process of designing a system that can be claimed to be secure. At the beginning of this process the participants of an informational activity are supposed to form a community. Each participant, or appropriate groups of them, expresses his specific needs and wishes for the computing system to be designed. Already on this level of abstraction, some conflicts among the participants' demands and with respect to informational (or other) rights may arise. After appropriately resolving these conflicts, all further steps are based on the fundamental

assumption that the intended purpose of the system is legitimate and consistent. Accordingly, on this level, we can tentatively define: *A system is* secure *iff it satisfies the intended purposes without violating relevant informational (or other) rights.*

Then, in further refinement steps, all the concepts have to be detailed and formalized, the already introduced concepts as well as further ones like the participants' interests and their anticipated threats or the trust in subsystems participants are willing to grant. We emphasize that all concepts are thought to be *decentralized.* Finally, at the end of the process, the definition of security roughly says that the final system meets the intended purposes, even if it is embedded in adversary environments, and it "does not do anything else" that has been considered to be harmful and has been explicitly forbidden therefor.

2.3 SELECTED MECHANISMS FOR TECHNICAL ENFORCEMENT

In Section 2.2.2 we considered informational assurances as comprising informational rights, social and legal rules as well as enforcing technical mechanisms. The technical enforcement mechanisms play a crucial rule in the routine cases of daily life, for the tremendous amount of technical informational events occurring within the information society can only be effectively controlled by means that are technical too. The technical enforcement mechanisms should make it technically infeasible to violate the social and legal rules, or otherwise, the mechanisms should effectively provide enough documented evidence against a violator. Then, the role of a human participant would be reduced to autonomously select technical enforcement mechanisms according to his rights and interests and the conflicts and threats anticipated by him, to control the selected mechanisms, and to use documented evidence of violations in (hopefully) exceptional and rare cases.

Evidently, these requirements appear to be difficult to meet, in particular because informational activities usually concern many participants with different expectations. There is some hope, however, to solve at least some aspects of this challenge by

- emphasizing federated (rather than centralized) system structures with a high degree of local security autonomy,
- employing cryptographic protocols (where cryptography is used as the discipline for enabling cooperation under threats), and
- using specialized hardware as tamper resistant foundation.

Of course, the indicated parts of such solutions refer to different layers of a computing system, and accordingly they would have to be carefully harmonized. Unfortunately, the author does not know about any comprehensive approach to such a solution. However, there are already a lot of proposals and subsystems for partial aspects available. In the rest of this section, some examples of them are shortly sketched, and their potential impact for a comprehensive solution is roughly indicated. The selection of the examples is strongly biased by the

author's personal experience, and the readers are cordially invited to add their own insight and contributions.

2.3.1 Federated system structure and local security autonomy

2.3.1.1 The paradigm of communicating personal data agents. Currently we can identify two extreme kinds of storing personal data. The first one uses traditional, centralized, and (more or less) well-structured databases which gather and hold all the data that the database owners suppose to need as data consumers for their organizational purposes, actually right now or potentially in the future. The second one is the rapidly evolving, totally decentralized, and (more or less) unstructured World Wide Web, WWW, where individuals or institutions offer their data as data providers for anyone who might take advantage from it.

The privacy legislation, as discussed in Section 2.1.1, deals with the first kind only. It attempts to protect individuals, acting as data providers, against the database owners that have physical control over the stored data. Among others, the protection is based on postulating a restriction: any supply of personal data for a database is bound to a specific, well-described purpose, and afterwards the database owners are not allowed to use that data beyond the stated purpose. As mentioned before, in this scenario the data subjects are in a somehow weak position, since they do not dispose of technical mechanisms to enforce the postulated restriction.

In order to remedy this situation, many years ago we designed and prototyped the so-called "personal model of data" [3, 4, 5, 13] that anticipated some of the innovative services that are now feasible by the WWW (and some more indeed, including roles, decentralized access control, and set oriented query processing). The basic approach of the personal model of data, as well as of the WWW, is that an individual as data subject retains full technical control over the storage of his data, which is locally held on a computing system of his choice and under his supervision and auditing. Surely, a participant that traditionally would own and maintain a database for his purposes still needs personal data, and thus we have to provide the appropriate means for this requirement. In the personal model these means are roughly layered as follows.

Firstly, the participant must hold an *"authority"* which can be interpreted as the access right (in today's CORBA terms a credential [39]) to execute the commands necessary to pursue the purpose in question. Secondly, the participant must be *"acquainted"* with the data subject in the sense that the participant knows the data subject's unique identifier in the network (in today's WWW terms the URL), in order to be able to direct the data request appropriately. Thirdly, we need the informational infrastructure which allows on-line procedures of the sort sketched here. And finally, after an autonomously performed access control and auditing action, the data subject's computing system has to correctly react indeed by transmitting the requested data.

This shift from the traditional paradigm of reference books implemented as centralized databases to the proposed paradigm of communicating personal

data agents already happens everyday in some sectors of the information society. These sectors are characterized by the supposed joint interest of data providers and data consumers to cooperate, in particular by the consumer's expectation and trust that requested data is properly provided whenever the request is legitimate. In other sectors, the consumer's concern on the *availability* of data still prevails the data provider's concern on *confidentiality* and control, as postulated by the principle of informational self-determination.

Interestingly, for both paradigms the concern on *integrity* of data turns out to be subtly distributed over both sides, and it strongly depends on the mutual trust among data providers and consumers (and infrastructure providers). Indeed, in the framework of informational assurances, both for availability and integrity, the new paradigm would demand for new legal rules and technical enforcement mechanisms in order that the data providers and their computing systems always cooperate as expected.

Whereas within the paradigm of communicating personal data agents a data subject retains full technical control over the *primary storage* of his data, he would still be left with some of the problems related to *using* that data once it has been communicated. Hence that paradigm would have to be complemented by further legal rules and enforcement mechanisms. The legal rules should disallow to permanently store communicated personal data, at least in a large scale (while demanding its mandatory availability on necessary demand at the data subject's site). And we could develop technical enforcement mechanisms for controlling the usage of personal data by exploiting techniques that have been introduced for digital money and electronic commerce (cf. e.g. [12, 56]), for instance fingerprints against unauthorized passing of electronic goods or measures against double spending of coins (see Section 2.3.2 below).

Reviewing the observations concerning the technical difficulties with the principle of privacy, as discussed in Section 2.1.1, we see that the new paradigm could offer promising solutions to many of them, but the fourth difficulty related to data about social relationships would remain, unless we could additionally find new forms of cooperative data representation and access control.

2.3.1.2 Federated database systems and mediated information systems. Besides the two extreme kinds of storing personal data we see also further informational services, in particular federated database systems [37, 52] and mediated information systems [57, 58]. Both services introduce new layers between the data providers and the data consumers, in order to assist participants of the information society in dealing with the increasing scope and complexity of information management. Obviously these additional layers also challenge us with respect to informational assurances. Most work for federated database systems has been devoted to resolving the heterogeneity of access rights among the components allowing them to perform access control widely autonomously, see for example [2, 23, 26, 33, 34]. Some recent work for mediated information systems also deals with the necessary trust in the intermediate layers and related problems [9, 22]. The work in both fields is apparently done

under the implicit assumption of a relative small number of components. It would be necessary to explore to which extent the results can be scaled for the tremendous number of participants in a system of communicating personal data agents.

2.3.1.3 Trust in certificates. In federated systems participants want to autonomously decide on their trust in *certificates*, as they are required, among others, for the public keys, which are used for verifying digital signatures or for encrypting confidential messages. Like for any other problem of informational assurances we have to consider the impact of many viewpoints. Of course, one viewpoint is the status of legal regulations. As presented in Section 2.2.5 and Section 2.2.6, there is substantial progress with respect to digital signatures, but, unfortunately, due to political debates on the conflicting goals of national security and law enforcement, not for encryption yet. Another viewpoint is the design of actual systems. Here we see already established systems like "Pretty Good Privacy", PGP [59], for enabling participants to autonomously employ end-to-end cryptography, both for signatures and encryption, or system specifications like CORBA [39], for allowing autonomous access control in federated object systems.

At the bottom of any consideration, a specific user has to evaluate to what extent he is willing to trust a certificate. Since such a certificate may be generated by a chain of actions of diverse participants, whether along hierarchies or within a "web of trust", the task of trust evaluation is quite subtle. One may wonder whether this task can be technically supported at all, because it mostly deals with social relationships. On the other hand, the mass of daily electronic transactions could require to elaborate on a formal model to automate routine decisions. A specific proposal for such a model and a discussion of other approaches can be found in [38].

2.3.2 Some cryptographic protocols enabling cooperation under threats

Cryptography can be considered as the discipline in computing which aims at cooperation under threats. If used in a decentralized fashion, as enabled by the asymmetric cryptography, it allows individuals to technically enforce many of their informational interests, including confidentiality, detection of loss of integrity, authenticity and non-repudiation. It must be emphasized, however, that asymmetric cryptography must be firmly founded in both the (more or less social) trust in certificates for public keys, as discussed before, and in tamper resistant hardware devices, considered below in Section 2.3.3.

This presentation is not the place to survey cryptography what has excellently been done for instance by [50]. Here we only mention some selected work that aims at providing documented evidence on happened events and on anonymity. Both features are important for the technical enforcement of informational assurances, and it would be worthwhile to exploit their potentials for the specific problems of privacy, in particular within the paradigm of communicating personal data agents.

Fail-stop signature schemes [40, 42] are a new class of digital signature schemes, which improve previously known schemes in case that somebody (unexpectedly) succeeds in forging a signature. Of course, such an unhappy event should not occur, but, unfortunately, we cannot totally exclude the possibility. For the security (in terms of unforgeability) of all known schemes is based on unproven assumptions in the theory of computational complexity, in particular on the famous assumption $P \neq NP$. Now, if a forgery actually happened for a fail-stop signature scheme, then a claimed but not actual signer can prove that forgery by demonstrating that the complexity assumption has been broken. The innovative signing protocol just delivers the necessary evidence to convince a court about this fact, and thus such a protocol can strengthen the situation of a (socially weak) signer against a (socially powerful) verifier.

Informational cooperation may require to exchange digital goods or to digitally sign contracts. The exchange or signing scheme must be fair in the sense that, even if one of the participants misbehaves, either both participants or none of them obtain what they expected. The classical pessimistic way is to ask a third party for assistance but at the price of extra costs. Optimistic exchange and contract signing schemes [1, 44] reduce that costs in that the third party is not actively involved in the fault-less case. Thus optimistic schemes are more suitable for the daily routine cases but still provide enough evidence for solving disputes in hopefully exceptional cases. If we consider personal data as a digital good which is provided on the basis of contracts, we could exploit such schemes for the paradigm of communicating personal data agents.

As mentioned before, privacy implies that a data subject retains control over both the primary storage of personal data and its usage once it has been provided to some consumer. For ordinary digital goods like copyrighted documents or software as well as for personal data a particular challenge is to control unauthorized proliferation. Again the provider is interested in producing some non-repudiatable pieces of evidence that he has delivered a specific copy of the item to a specific receiver. Recent progress on asymmetric fingerprinting schemes [45, 46, 47] already achieves this goal for large electronic goods like pictures.

Fingerprinting cannot prevent the passing of data but can only deter participants to transmit data if not authorized. Technically enforced strict prevention has been studied in the framework of digital money in order to avoid the double spending of electronic coins. On-line prevention techniques restrict the availability of the informational services under consideration and the autonomy of the participants. Off-line prevention appears to require what has been called "wallets with observers" [21]. The "observer" is an electronic substitute of that participant that has an interest in controlling an electronic action of another participant. That substitute is physically implanted into the computing device of the participant to be controlled. In case of electronic coins, the observer is the substitute of the bank that wants to control its client. This scenario assumes that the controlling participant (the bank) can oblige the controlled participant (the client) to use the customized tamper resistant computing de-

vice with the implanted observer for the informational cooperation (spending a coin). Surely this scenario is completely different from the privacy scenario where everybody would act as a controlling participant regarding any receiver of his data as a participant to be controlled. So, obviously we are still far away from the ultimate goal of privacy.

The seminal work of [19, 20] introduced the possibility of anonymity and digital pseudonyms for informational cooperation. Surely these features could be very important for the field of health care when personal data is required to be provided beyond the protected environment of professional secrecy, which is constituted by the special relationship of a patient and a physician or other persons directly caring for the patient. Then confidentiality and privacy requirements on the one side could be maintained while also supporting other interests like fair clearing procedures for health care providers and health insurances on the other side. A first study of feasibility [10, 11] has shown that both features could be achieved indeed. Surely, before introducing the proposed new schemes we would have to study the technical details as well as the social implications more deeply.

Digital pseudonyms allow non-observability of a participant's behaviour on the application layer. On the communication layer, we would also like to protect participants against observing their activities on the communication network, i.e., their sending and receiving of messages. This goal can be achieved to some extent by so-called mixes [19, 32]. In a mix communication network each exchange node is organized as a mix where on each round messages are gathered, cryptographically recoded (decrypted and reencrypted), resorted, and retransmitted. As a result, adversary observers cannot trace messages travelling through the network.

2.3.3 Tamper resistant hardware foundation

Any technical enforcement mechanisms have to be founded somehow within the hardware. In particular, if a participant wants to enforce his interests by some cryptographic scheme then his protection crucially depends on his reliable control over generating, storing and using the secret keys. For this purpose he needs a personal computing device, which in particular physically isolates the cryptographic secrets. These devices must be tamper resistant in the sense that they are physically protected against unauthorized attempts to read or modify their contents, the secrets as well as their programs.

Again many viewpoints have to be considered, see e.g. [41] for a recent discussion. Among them are legal and social rules for manufacturing and distributing such devices, and both rules and technical measures for dealing with loss or theft of such devices. Since the devices are devoted to informational cooperation with other participants, also their potentially conflicting interests have to be honoured. The "observers", mentioned in the preceding Section 2.3.2, are an example of providing a physically implemented electronic substitute of those participants.

2.4 A SUMMARY WITH RESPECT TO PRIVACY

I advocate considering the issue of privacy within a more comprehensive framework of informational assurances, which take care of both restricting and enabling participation in the "information society". The informational assurances include technical mechanisms enforcing pertinent laws and related social and legal rules. As far as possible at all, technical mechanisms should be physically controlled by those participants whose interests are enforced.

Privacy, understood as informational self-determination, demands control over the primary storage, the transmission and the usage of personal data and over the knowledge about personal behaviour within the computing system under consideration.

Control concerning personal data seems to be best achievable if we treat personal data like any other electronic good in electronic commerce. Then personal data would be primarily stored in personal data agents, which communicate on demand. An agent transmits data if and only if required by the consumer and autonomously agreed on by the supplier who controls the agent. Transmission of personal data would be only one part of a more comprehensive electronic transaction of contract signing and fair exchange. Exploiting techniques developed for electronic commerce, like digital signatures, fingerprinting, "observers" and others, a data subject could be provided with technical means to control usage of his data once it has been transmitted, in particular by producing non-repudiatable pieces of evidence to deter the misuse of data.

Control over knowledge about personal behaviour require informational services which allow anonymity and digital pseudonyms. These services have to be offered on the application level and on the communication level. While on the application level an individual can have the direct disposal of his anonymous or pseudonymous credentials, on the communication level network providers can only be indirectly and socially supervised.

Acknowledgments

I sincerely thank U. Flegel, R. Menzel and T. Polle for carefully reading draft versions and helping to improve the presentation. I am also grateful to K. Rannenberg for valuable hints.

References

[1] N. Asokan, M. Schunter, M. Waidner, Optimistic protocols for fair exchange, In: Proc. 4th ACM Conference on Computer and Communication Security, Zürich, 1997, pp. 6–17.

[2] Bertino, E., Buccafurri, F., Ferrari, E., Rullo, P., An authorization model and its formal semantics, Proc. 5th European Symposium in Computer security, ESORICS, 98, Sept. 1998, Lecture Notes in Computer Science, Springer, Berlin etc., to appear.

[3] J. Biskup, Privacy respecting permissions and rights, In: C. E. Landwehr (editor), Database Security : Status and Prospects, North-Holland, Amsterdam etc., 1988, pp. 173–185.

[4] J. Biskup, H. H. Brüggemann, The personal model of data, Computers & Security 7,6 (1988), pp. 575–597.

[5] J. Biskup, H. H. Brüggemann, Das datenschutzorientierte Informationssystem DORIS: Stand der Entwicklung und Ausblick (in German), In: A. Pfitzmann, E. Raubold (editors), Proc. VIS '91 – Verläßliche Informationssysteme, Springer, Berlin etc., 1991, pp. 146–158.

[6] J. Biskup, Sicherheit von IT-Systemen als "sogar wenn – sonst nichts – Eigenschaft" (in German), In: Proc. GI-Fachtagung Verläßliche Informationssysteme – VIS'93 (G. Weck, P. Horster, editors), DuD Fachbeiträge 16, Vieweg, Wiesbaden, 1993, pp. 239–254.

[7] J. Biskup, G. Bleumer, Reflections on security of database and datatransfer systems in health care, In: Proc. 13th World Computer Congress 94, Volume 2 (K. Brunnstein and E. Raubold, editors), Elsevier Science (North Holland), Amsterdam etc., 1994, pp. 549–556.

[8] J. Biskup, G. Bleumer, Cryptographic protection of health information: cost and benefit, International Journal of Bio-Medical Computing 43 (1996), pp. 61–67.

[9] J. Biskup, U, Flegel, Y. Karabulut, Secure mediation: problems and design, In. Proc. IFIP WG 11.3 Workshop on Database Security, Chapman & Hall, London etc., 1998, this volume.

[10] G. Bleumer, M. Schunter, Privacy oriented clearing for the German health care system, In: R. Anderson (editor), Personal Information Security, Engineering and Ethics, Springer, Berlin etc., 1997, pp. 175–194.

[11] G. Bleumer, M. Schunter, Datenschutzorientierte Abrechnung medizinischer Leistungen (in German), Datenschutz und Datensicherheit 21,2 (1997), pp. 88–97.

[12] J. P. Boly et al, The ESPRIT project CAFE—high security digital payment systems, In: D. Gollmann (editor), Computer Security—ESORICS 94, Proceedings of the 3rd European Symposium on Research in Computer Security, Lecture Notes in Computer Science 875, Springer, Berlin etc., 1994, pp. 217–230.

[13] H. H. Brüggemann, Interaction of authorities and acquaintances in the DORIS privacy model of data, In: Proc. 2nd Symposium on Mathematical Fundamentals of Database Systems, Lecture Notes in Computer Science 364, Springer, Berlin etc., 1989, pp. 85–99.

[14] Der Bundesbeauftragte für den Datenschutz, Bundesdatenschutzgesetz – Text und Erläuterung (in German), Bonn 1991.

[15] Bundesverfassungsgericht, Urteil vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 (in German), Bundesanzeiger 35,241a, 1983.

[16] Canadian System Security Center, Canadian Trusted Computer Product Evaluation Criteria, Version 3.0, Jan. 1993.

[17] Commission of the European Communities, Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, June 1991.

[18] Common Criteria Editorial Board, Common Criteria for Information Technology Security Evaluation, Version 1.0, Jan. 1996 (for Version 2, May 1998, see `http://csrc.nist.gov/cc`).

[19] D. Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, Communications of the ACM 24,2 (1981), pp. 84–88.

[20] D. Chaum, Security without identification: transaction systems to make big brother obsolete, Communications of the ACM 28,10 (1985), pp. 1030–1044.

[21] D. Chaum, T. P. Pedersen, Wallet databases with observers, In: Proc. Crypto '92, Lecture Notes in Computer Science 740, Springer, Bonn etc., pp. 89–105.

[22] S. Dawson, S. Qian, P. Samarati, Secure interoperation of heterogeneous systems: a mediator-based approach, In: Proc. IFIP SEC 1998, Chapman & Hall, London etc., 1998, to appear.

[23] S. De Capitani di Vimercati, P. Samarati, Authorization specification and enforcement in federated database systems, Journal of Computer Security 5,2 (1997), pp. 155–188.

[24] Deutsche Bundesregierung, Signaturverordnung, Oct. 1997 (see `http://www.iid.de/iukdg` for the German text and an English translation).

[25] Deutscher Bundestag, Informations- und Kommunikationsdienste-Gesetz, Bundesgesetzblatt I S.1870, 1997 (see `http://www.iid.de/iukdg` for the German text and an English translation).

[26] W. Eßmayr, G. Pernul, A. M. Tjoa, The security API of IRO-DB, In: S. Katsikas (editor), Communications and Multimedia Security Vol. 3, Chapman & Hall, London etc., 1997, pp. 178–189.

[27] European Commission, Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data, 1995.

[28] European Commission, Towards a European framework for digital signatures and encryption, Communication COM (97) 503, Oct. 1997 (see `http://www.ispo.cec.be/eif/policy`).

[29] European Commission, The need for strengthened international coordination, Communication COM (98) 50, Feb. 1998 (see `http://www.ispo.cec.be/eif/policy`).

[30] European Commission, Directive on a framework for the use of electronic signatures, Proposal COM (98) 297, May 1998 (see `http://www.ispo.cec.be/eif/policy`).

[31] H. Fiedler, Informationelle Garantien für das Zeitalter der Informationstechnik (in German), In: M.-T. Tinnefeld, L. Philipps, and K. Weis (editors), Institutionen und der Einzelne im Zeitalter der Informationstechnik, Oldenbourg, München-Wien, 1994, pp. 147–158.

[32] E. Franz, A. Jerichow, A. Pfitzmann, Systematisierung und Modellierung von Mixen (in German), In: G. Müller, K. Rannenberg, M. Reitenspieß, H. Stiegler (editors), Verläßliche IT-Systeme – Zwischen Key Escrow und elekronischem Geld (Proceedings der GI-Fachtagung VIS '97), Vieweg, Braunschweig-Wiesbaden, pp. 171–190.

[33] Jajodia, S., Samarati, P., Subrahmanian, V. S., Bertino, E., A unified framework for enforcing multiple access control policies, Proc. ACM SIGMOD Int. Conference on Management of Data, May 1997, pp. 474–485.

[34] D. Jonscher, K. R. Dittrich, An approach for building secure database federations, In: Proc. 20th VLDB Conference, Santiago, Chile, 1994, pp. 24–35.

[35] W. Kilian, Europäisches Datenschutzrecht – Persönlichkeitsrecht und Binnenmarkt (in German), In: M.-T. Tinnefeld, L. Philipps, and S. Heil (editors), Informationsgesellschaft und Rechtskultur in Europa, Nomos, Baden-Baden, 1995, pp. 98–109.

[36] C. Laske, Legal issues in medical informatics: a bird's eye view, In: B. Barber, A. Treacher, C. P. Louwerse (editors), Towards Security in Medical Telematics—Legal and Technical Aspects, IOS Press, Amsterdam etc., 1996.

[37] W. Litwin, L. Mark, N. Roussopoulos, Interoperability of multiple autonomous databases, ACM Computing Surveys 22:3 (1990), pp. 267–293.

[38] U. Maurer, Modelling a public-key infrastructure, In: E. Bertino, H. Kurth, G. Martella, E. Montolivo (editors), Computer Security—ESORICS 96, Proceedings of the 4th European Symposium on Research in Computer Security, Lecture Notes in Computer Science 1146, Springer, Berlin etc., 1996, pp. 325–350.

[39] OMG (Object Management Group), CORBA Security, OMG Document 96-08-03 through 96-08-20, July 1996.

[40] T. Pedersen, B. Pfitzmann, Fail-stop signatures, SIAM Journal on Computing 26,2 (1997), pp. 291–330.

[41] A. Pfitzmann, B. Pfitzmann, M. Schunter, M. Waidner, Trusting mobile user devices and security modules, IEEE Computer 30,2 (1997), pp. 61–68.

[42] B. Pfitzmann, Digital Signature Schemes—General Framework and Fail-Stop Signatures, Lecture Notes in Computer Science 1100, Springer, Berlin etc., 1996.

[43] B. Pfitzmann, M. Waidner, A general framework for formal notions of "secure" systems, Hildesheimer Informatik-Berichte 11/94, Universität Hildesheim, 1994.

[44] B. Pfitzmann, M. Schunter, M. Waidner, Optimal efficiency of optimistic contract signing, IBM Research Report RZ 2994 (#93040) 20/04/98.

[45] B. Pfitzmann, M. Schunter, Asymmetric fingerprinting, In: Proc. Eurocrypt '96, Lecture Notes in Computer Science 1070, Springer, Berlin etc., 1996, pp. 84–95.

[46] B. Pfitzmann, M. Waidner, Kopierschutz durch asymmetrische Schlüsselkennzeichnung mit Signeten (in German), In: G. Müller, K. Rannenberg, M. Reitenspieß, H. Stiegler (editors), Verläßliche IT-Systeme – Zwischen Key Escrow und elekronischem Geld (Proceedings der GI-Fachtagung VIS '97), Vieweg, Braunschweig-Wiesbaden, pp. 17–32.

[47] B. Pfitzmann, M. Waidner, Asymmetric fingerprinting for larger collusions, In: Proc. 4th ACM Conference on Computer and Communications Security, Zürich, 1997, pp. 151–160.

[48] K. Rannenberg, Recent development in information technology security evaluation—The need for evaluation criteria for multilateral security, In: R. Sizer, L. Yngström, H. Kaspersen, S. Fischer-Hübner, Security and Control of Information Technology in Society, Proceedings of the IFIP TC9/WG 9.6 Working Conference, aboard M/S Ilich and ashore at St. Petersburg, Russia, August 12–17, 1993, North-Holland, Amsterdam, pp. 113–128.

[49] K. Rannenberg, Zertifizierung mehrseitiger IT-Sicherheit – Kriterien und organisatorische Rahmenbedingungen (in German), Vieweg, Braunschweig-Wiesbaden, 1998.

[50] B. Schneier, Applied Cryptography (2nd Edition), Wiley & Sons, New York etc., 1996.

[51] The SEISMED Consortium, Data Security for Health Care, Vol. I (Management Guidelines) + Vol. II (Technical Guidelines) + Vol. III (User Guidelines), Studies in Health Care and Informatics 31–33, IOS Press, Amsterdam etc., 1996.

[52] A. P. Sheth, J. A. Larson, Federated database systems for managing distributed, heterogeneous and autonomous databases, ACM Computing Surveys 22:3 (1990), pp. 183–236.

[53] S. Simitis, U. Dammann, Körner (editors), Data Protection in the European Union—The Statuary Provisions, Nomos, Baden-Baden, 1992.

[54] S. Simitis, Vom Markt zur Polis: Die EU-Richtlinie zum Datenschutz (in German), In: M.-T. Tinnefeld, L. Philipps, and S. Heil (editors), Informationsgesellschaft und Rechtskultur in Europa, Nomos, Baden-Baden, 1995, pp. 51–70.

[55] US Department of Defense, Trusted Computer System Evaluation Criteria (Orange Book), Dec. 1985.

[56] M. Waidner, Development of a secure electronic marketplace for Europe (SEMPER), In: E. Bertino, H. Kurth, G. Martella, E. Montolivo (editors),

Computer Security—ESORICS 96, Proceedings of the 4th European Symposium on Research in Computer Security, Lecture Notes in Computer Science 1146, Springer, Berlin etc., 1996, pp. 1–14.

[57] G. Wiederhold, Mediators in the architecture of future information systems, IEEE Computer 25:3 (1992), pp. 38–49.

[58] G. Wiederhold, M. Genesereth, The conceptual basis for mediation, IEEE Expert, Intelligent Systems and their Applications 12:5 (1997), pp. 38–47.

[59] P. R. Zimmermann, The Official PGP User's Guide, MIT Press, Boston, 1995.