Legal Aspects of Mobile Agents

With special consideration of the proposed Austrian E-Commerce Law

Michael Sonntag
Institute for Information Processing and Microprocessor Technology (FIM)
Altenbergerstr. 69
A-4040 Linz
Austria
email: sonntag@fim.uni-linz.ac.at

Abstract

Legal aspects of (especially mobile) agents, which are a special case or improvement on components, have previously been rather neglected. With agents maturing and finding more applications this area increases in importance. We will take a look at some legal and technical (for providing evidence) questions and relate them with the proposed Austrian E-Commerce law, which in the paragraphs concerned is closely following the EU E-Commerce directive. Therefore these thoughts have a wider area of application. We will explain liability for acts of agents, receipt of statements, how to prove that an agent received some information and electronic signatures by agents. At the end some important open questions will be listed.

1 Introduction

Agents are a special form of (or improvement on) components. They are goal directed and usually self-activating in the sense, that they possess their own thread of execution and can initiate actions without intervention from the outside (incoming communication, user interface, ...). An important distinction between agents and components (on which they are usually based for implementation) is, that agents can decide, whether to fulfill requests made to them, while components just execute commands. This means, an agents may or may not execute commands at his discretion (internal state, goals, etc.), while standard components do not have this possibility: Their code is always just executed. A special subset of agents are mobile agents, which can travel from one host to another, taking their code, data, and state with them.

Because of this mobility a number of legal problems can arise. Stationary agents, which always remain on the server on which they were created, are less of an issue: They remain completely under the control of their owner if locally created (see Figure 1). If created on a remote computer (different from the computer the person directing the agent works on; see Figure 2), the owner of this host could at least decide whom he allows this privilege, and which code or parameters are allowed. Mobile agents, however, are perhaps executed on a host, which has nothing at all to do with the agent or its owner (see Figure 3). It need not even be a prospective business partner.

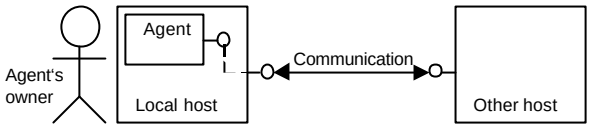

Figure 1: Local agent with remote communication

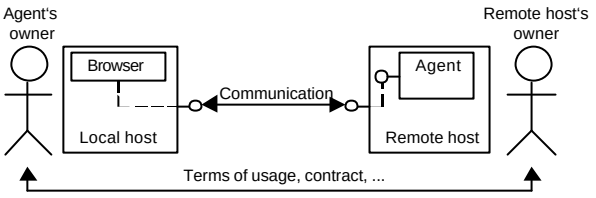

Figure 2: Agent created at remote host

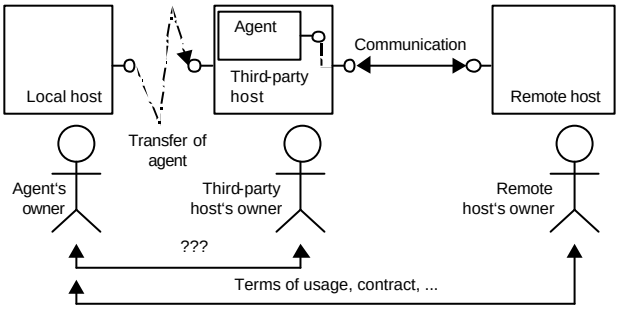

Figure 3: Mobile agent, transferred to a third-party host

For some problems, technical solutions are available, but these only serve to provide evidence and in some rare cases prevent problems. Legal issues (to a lesser extent security measures) are mostly ignored, usually because only closed systems are developed (e.g. [Aglets]). In such systems (e. g. inside a company) it is rather easy to set a standard of action and enforce consequences of misconduct. However, if agents are to be released into an open system like the internet (e.g. [POND]), this no longer works and the importance of legal enforceability increases. This is even more a problem if agents carry valuable information (E-Cash, credit card numbers, etc.) or are used in E-Commerce where real money is at stake.

We will therefore take a look at some selected issues of mobile agents and discuss their legal consequences as well as what can be done to ensure success in an eventual dispute. Special attention is given to the proposed Austrian legislation (E-Commerce law or ECL, [ECL-Draft]), which is closely based on the E-Commerce directive (ECD) of the EU ([ECD]).

2 Legal classification of actions of agents

Before taking a look at the actions of agents we must ask what an agent is, seen from a legal point of view. An agent is neither a natural nor a legal person but just a tool, regardless of its autonomy and abilities. It can therefore never legally „act" on its own, and is always an extension of one or more persons. Of the acts of agents two types are of special interests: If the agents acts result in some kind of damage, who is liable for it; and whether an agent is able to conclude a contract.

2.1 Liability for agents acts

The question, who is liable for a mobile agent's acts, needs closer attention and depends also on the action considered. Four persons are possible: The network provider, where the agent is transported, the creator of the agents code, the person providing the parameters (the owner) and the operator of the server, the agent is executed on.

Network provider: The network operator has usually no contract with any of the other parties involved. He can be liable for damages only in case of intentional modifications of the transmission (see § 14 ECL, Art 12 ECD, where this is a general rule; some restrictions apply). This is of lesser importance, as through encryption and electronic signatures effective detection of attacks during transmission is possible.

Programmer of the agent's code: The creator of the code of an agent might be in a bit of a different legal position compared to a provider of a conventional component. The latter has usually no connection and no obligations towards third parties (other than the buyer of the component), while the creator of a mobile agent might have such. In this case a contract with protection of third persons („Vertrag mit Schutzwirkung zugunsten Dritter"; [Koziol/Welser 2001] 135ff) is possible. This applies, if because of the contract third persons (different from the parties to the contract) are especially endangered and those persons belong to the sphere of interest of one of the parties. If the code is defective, owners of servers the agent moves to are especially threatened, because their computers (or the base agent system) might crash, or resources (e. g. processor time, memory) are exhausted. On the other hand this is a very large and potentially unlimited number of persons, where only very loose ties to one partner (often no contract or actual proximity, like family members) exists, so enlarging the liability to them is probably excessive. Moreover, only damages which are not only loss of assets would be covered by this (destruction of objects, injuries of persons, …), which is very unlikely. We can therefore summarize that the creator of the code of a mobile agent is only liable to the owner of the agent, who licensed or bought it. Towards third persons, only liability for offenses exists, which is rather limited (most important: intentional unethical damages, § 1295 para. 2 ABGB).

Owner of the agent: Because of an agent's autonomy, the results of actions depend much more on the parameterization of the code compared to ordinary software. Agents can, because of their universality, do damage by being „tricked" into otherwise harmless actions by clever combinations of parameters. On the other hand, because of this flexibility individual activity might be very hard to predict. For the liability to third persons, e.g. owners of servers, this is not of importance. The owner of the agent uses it to fulfill his own goals and is therefore liable for of breach of (a in most cases tacit or explicit) contract for all damages the agent causes. The differentiation between the programmer and the user of the code is much harder. Three areas exist: Problems which are solely because of the code (e. g. bugs causing the agent to crash) are the liability of the programmer, while problems with input values (goals, parameters; e. g. wrong configuration) must be associated with the owner. The middle area, where the code and the parameters are correct but an undesired result appears, is difficult because it is based on some kind of misunderstanding of the working of the agent.

The agent's code, like all components, must be accompanied by an extensive documentation, where the interpretation is to be judged according to a typical computer user with the special knowledge of the actual user. This documentation will usually not be part of the actual contract (when buying a car, the complete specification is also not part of the contract), but be more than just a handbook. The documentation is an indispensable part for using a component: It often requires other components, which must be of certain types, and extensive customization by the user is essential. It is an integral part of the main subject of the contract and not only an additional secondary part.

An agent as a component is a special case in regard of the legal type of its specification. Standard software only has to fulfill the (rather low) general expectations for software of this type as well as the features, which are explicitly stated. A contract for buying this type of software is therefore rather short. In contrast to this, a contract for individual software usually contains an extensive list of all features and capabilities the software should possess, and is therefore long. This specification is a full part of the contract. When acquiring an agent, no general expectation exists, which could serve as a base, and a widely understandable description of its workings will only be extremely rough, because of agents multiple ways of solving their tasks. Also, the agent itself is not usable alone. Additional software (at least a base system, but probably other agents as well) are needed and the actions of the agent may depend largely on this environment. This disallows a complete documentation other than the full source code because of the resulting huge size. The documentation of an agent must therefore be rather gen-

eral (but detailed) and will be often part of the contract. Even if it is not contained in the contract it will be enforceable, because it is the base of it and describes what the subject of the contract is exactly.

Server owner: The owner of a server has a higher standard compared to a network provider, as he is, to a certain extent, also liable for the information stored. According to § 16 ECL/Art 14 ECD a hosting provider is not liable, if he has no positive knowledge of illegal activities or data and also knows of no facts or circumstances, which obviously point in this direction. If he receives knowledge he has to immediately remove the offending data or terminate access to it. In the context of agents this means that the servers owner is not liable for any information stored within the agent as long as he is ignorant of it (e. g. not, when buying this information or when a faked certificate is presented). The „knowledge" of the server is attributed to the owner, so the agent system must check for obvious hints a human in its place would recognize. It should be noted that these legal requirements also apply to providers which offer their services without any charge or contract with a user (§ 20 para. 2 ECL). As the „activity" of an agent is an extension of its owner, any illegal action of an agent is also cause for these consequences. However, the standard for suspicious circumstances will be rather low as no obligation for surveillance exists (§ 19 para. 1 ECL; a provider need not monitor his users or investigate on his own for possible illegal activities). In contrast to this, some hints from the security system have to be taken seriously, e. g. when repeated security exceptions occur, because actions are tried which are forbidden to the agent. Problematic is, that the provider shall ascertain whether some act or information is illegal: This is usually the domain of courts and wrong assessment might lead to consequences for the owner. A different interpretation could solve the problem: the „knowledge" not only applies to the act, but also to the illegality of it. Other issues in this connection are the consequences: The owner should remove the information or prevent access to it. The idea behind this rule was information stored on webpages, which can be easily taken offline without additional problems. In the case of a mobile agent this does not work. The only options are to either leave the agent as it is (not covered by the law), send it home (also not covered by the law; not even the author/owner should get access any longer), terminate it (stop its threads and destroy them) or just stop it. The last two possibilities are both valid. Completely destroying it is an equivalent of removing the information, as only logs remain as evidence for possible legal actions. Just stopping its thread and saving the state equals preventing access to the data, while leaving behind evidence. This last response is therefore preferable and destroying an agent should only take place if the agent was stopped a long time ago (cleaning up) or keeping copies would place too large a burden on the server (e. g. for very large and highly frequented servers). A notification of the agent's owner is not required, but advisable: if the agent was stopped erroneously, this reduces the damage (just stopping the agent allows resuming it later).

2.2 Representation through agents

The second issue of agents concluding a contract also depends on the agent being a tool. It can therefore never be a proxy in a legal sense (only possible by persons, not through tools), but is just a messenger (delivering its owner's statements). However, several questions arise:

Awareness of giving a statement: With an agent's autonomy, not every action or statement by them is exactly foreseen and planned by its owner. We must therefore ask, whether these statements are legally binding. In Austria awareness is of no importance if three prerequisites are fulfilled: First, the person issuing the statement must have adequately caused it. Second, the issuer must have been able to avoid, that the other party understands it as a statement. Third, the receiving party actually relied on it. Starting the agent with a task and sending it to another host is sufficient cause. By not using it he could have avoided any misunderstanding by the recipient. So if the server or another agent did rely on a message of an agent, the owner of the agent is legally bound to it.

Validity of using electronic communication (§13 para. 1 ECL): According to the proposed law statements can be made by E-Mail or „similar means of individual electronic communication". Although agents could use E-Mail, the common type of communication between agents of different owners will be message passing. These messages are individually addressed and are essentially the same as an E-Mail message (asynchronous and personally addressed). The main difference is that it might not be readable by a human. However, E-Mail also encompasses HTML pages as content or attachments of any type, so this difference does not matter. Another provision in this paragraph allows this type of communication only if the sender can expect the recipient to accept messages transmitted in this way. This is typically the case in replies (the other party started the communication in this way). In connection with agents this acceptance can be assumed by default, as it is the typical mode of communication. The last part of this provision might be a problem: The parties must ensure that statements are viewable and readable (so the other can understand them). Communication between agents must therefore use a mutually agreed form of communication (some standard, e. g. [KQML], [KIF], [FIPA]) or are legally seen as not being delivered to the recipient. The biggest problem is that between corporations and end-users agreements over the use of electronic communication must be individually negotiated (§ 13 para. 1 ECL). Mentioning them in terms of business is not sufficient. According to the explanations of the law, this should be seen in accordance to § 6 para. 2 KSchG[1], where certain clauses are only valid if they were individually negotiated. This requires discussion and the ability of the consumer to influence the wording of the clause. To allow a company therefore to enforce electronic communication (e. g. for delivering notices for termination), either an offline-agreement must be reached, or the agents must

[1] Konsumentenschutzgesetz, BGBl 1979/140 idF BGBL I 2001/48

separately discuss and agree on the terms. This has also been criticized in the comments on the draft.

Receipt of statements: When does a statement of e. g. the server reach the owner of the agent: When the agent receives it at the remote server, or when the agent arrives back home? § 11 para. 3 and § 13 para. 2 ECL define that a statement was received, if the recipient can access it. Important to note is, that this is independent of the time (previously receipt of E-Mail was seen as possible only during office hours or their beginning, see e. g. [Zankl 2001]; the same is explicitly said in § 13 AVG[2] [AVG] for communication with public authorities). For an exact definition the formula of „entering the sphere of the recipient" can serve. Because an agent is solely under the power of the server, it is unclear whether delivering it to the agent is sufficient. But the server cannot be held liable for actions of other hosts, which may be on the way before the agent returns home. For the latter cases, the agent can be seen as a messenger of its owner and therefore as part of his sphere. The critical point in time is therefore the moment, the agent successfully leaves the server, which sent the message. From there on the statement travels on the risk of the recipient. § 11 ECL requires the provider to immediately confirm the receipt of an electronic contract statement. However this does not apply to agents, as para. 4 states that this is not applicable if the contract is concluded solely by individual electronic communication, which is the case with agents. A confirmation (a message in return is sufficient) is required if the agent is sent in response to e. g. an offline-advertisement. As this is very difficult to detect, it should be sent anyway.

3 Proving that an agent received information

Currently an agent is still powerless against the host it resides on. It cannot hide data from it and the host could make every modification to its code and data it wants without the agent being able to even detect this. However, this problem also allows agents a special line of reasoning: Because they are powerless, they can always tell that the server did not fulfill a certain promise (e. g. delivering some information to the agent) or reverted the agent to a previous state. The owner of the host can never disprove this on his own.

A partial (only for ascertaining the knowledge at a certain point in time) solution for this problem is to do a signed „hand-off" (a simplified version of the protocol described in [Vigna 1998]) when an agent leaves a server. The recipient provides the sender with a signed digest of the code and the state of the agent he is receiving. This is an evidence for the server, that the agent was in a certain state at the time he left his area of power. A difficulty in this context is that with the signed digest alone no proof is possible. To prove a certain state a full copy of the agent must be retained for later inspection, whether the information is present in the agent and the signature matches the data. This requires the receiving server to store the whole data of the agent for a (probably) long and not exactly limited time. To create evidence for the state of the agent and continue working there, a solution similar to a secure timestamp could be used. The agent is „transferred" to another server and immediately moves back. This could be reduced to sending just the state and the code and receiving a signed stamp of the third-party server without terminating and recreating the agent. In contrast to timestamps (requires only signing a digest and the current time) this places a large burden on the third party, as the whole data received must also be stored. In a better version this exchange takes place with the home-host of the agent, which can be expected to cope better with this problem (it is his agent after all), or ignore it by just verifying the state and providing the signature without storing the serialized data.

Even if this signed exchange takes place, a further problem is possible: The agent could receive the information, but later on delete it before moving to another host. The result would be indistinguishable from the host never providing the information at all. A solution for this problem is to integrate a read-only store into agents which can only be written (and therefore items removed) by servers. In this way a host can deliver some information to an agent which will remain there regardless of an agents actions. With the signed digest from the receiving host later modifications are also not a problem for the original server.

An improvement could be made in this way that only a digest of a certain part (the interesting information) is signed and returned by the receiving server. This would require only a local copy of the information and the identity of the agent (to uniquely identify it and lock the association between those two). To allow this, the protocol for transferring an agent would need to be extended to allow specification of the parts for which a return receipt is required.

This concept of a read-only store accessible only by the server has an important drawback: A malicious host could fill up the store with some kind of data so that the agent gets very large, which is a drawback when moving (denial of service attack). Also, depending on the implementation, a slot that is reserved by the agent for certain data at a later point in time could be filled up so that then a collision occurs. The biggest problem is that a host could insert data without request by the agent and later demand payment for it, because it fulfilled its part of the (alleged) contract. An agent should therefore be able to deny access to the store (which is not really possible because of the basic problem!). A workaround for this problem would be to conclude a contract from a remote server (so there can be non-repudiable evidence for it) and then move there only for collecting the data. In this way no modifications are possible any more.

4 Electronic signatures by agents

An important part in concluding an electronic contract is applying digital signatures to messages or the contract

[2] Allgemeines Verwaltungsverfahrensgesetz 1991 - AVG BGBl 1991/51 (WV) idF BGBL I 137/2001

itself. When an electronic signature is legally equal to a handwritten signature is defined in the Austrian Signature Law ([SigL]), which is based in the EU Signature Directive ([SigD]). An agent can create a digital signature without any problem, but is this signature legally binding for its owner? According to the signature law and the signature ordnance ([SigO]) they are not. Only authorized software (by the signature services provider) may be used (which could be done for agents), but the components may also not store the authorization code for initiating a signature (SigO §7 para. 3). This would be a necessity because otherwise the agent could only serve as another piece of software used for signing (might be helpful in some rare cases).

However, agents can create normal digital signatures. This is sufficient in most cases, as the formal requirement for a signature is rather rare. Common contracts for sale of goods or services for example have no such requirement. The biggest drawback in this context is that the legal presumption on the correctness of the content of a signed document is not applicable. Signatures are explicitly allowed as evidence regardless how they were created (software, algorithms, …; SigL § 3 para. 2). Because of their technical security they will be rather important. But two cases have to be distinguished here: Signatures created on the home server, and those created on other servers. Signatures where the actual signing was done on another (untrusted) host are probably suspect, because the host could initiate the signing process, even if the agent itself would not. This also leads to the question to identify on which host the actual signing took place. This could be done either through secure timestamps and identifying through logs on which computer the agent was located at that time (rather complicated), or a countersignature by the server. Other hosts cannot forge this. The location of creation of not-countersigned signatures would have to be identified by logs (or hand-offs; see above).

In one special case a legally fully valid signature could be created. If the exact data (or more practically relevant, a checksum of it) to be signed is known, the signature can be created by the owner at home and taken with the agent. This is for example useful for providing a signed evidence of receipt. Without the knowledge of the exact data, this signature is not accessible: At home we create the signature to be delivered and encrypt it with a key deterministically created from the data itself (difficult in asymmetric encryption, but symmetric is sufficient here). From this the signature cannot be extracted (=decrypted) without the knowledge of the key, which depends on the data to be received. If the host has access to the data, he can decrypt and access the signature. That the agent really receives the data intended in exchange for the signature can be proved by the method outlined above. This works only for a relatively small area of applications because of the requirements: The data or its characteristics must be known exactly in advance (which, for example, disallows the usage of timestamps within it). This method has a wider range of applications, as it is independent of the data to be released at receipt of some information. Another application would be to encrypt E-Cash in this way, allowing access to it only in exchange for certain information (whichs description was presented to the owner at home, who thereafter encrypted the payment for it), but not otherwise.

In comparison to Europe, in the USA signatures by agents are legally accepted at least in some cases, e. g. the Electronic Signature Act [USElSigAct]. According to it, a contract may not be discriminated, because an electronic agent had some part in its creation or handling. This only applies if the action of the agent is legally attributable to the person to be bound. When this is the case is not stated. We may say that a signature by an agent on its home server will be fully valid, but if it is created on another server, special indications whether there were modifications by the server or that there were none might be required.

5 Open issues

Numerous questions in this area are still unanswered and need attention. Some of them are mentioned here:

- What are the legal consequences of mobile agents traveling through different countries? In contrast to ordinary internet traffic, they are not just transported, but probably executed on servers in other countries. If they possess some information, which is illegal in this country, but lawful in the countries of its origin and destination, could the agent be stopped? What actions are required with this information to constitute an offense, or is the mere existence sufficient?
- On a more technical side it is difficult to identify the server, which is responsible for the destruction or a certain change in an agent. Even if extensive logs are used following them is extremely expensive and difficult, especially if they are located on other countries (often a court order is required for disclosure).
- In some cases electronic signatures and logs would allow automatic arbitration with the evidence collected. However, what should be the result: a fine, an E-Mail to the parties, …, how would it be enforced?
- Similar to users on the web, the nationality of an agent is easily defined: Its owner's nationality. But how can this be detected and/or verified? Certificates are a possibility, but the nationality is usually not verified and included in them. This is especially important for blocking or disallowing some actions for agents of a certain nationality, e. g. to enforce taxes or not to sell certain goods to some countries. A solution could be using attribute certificates certifying the nationality, similar to the authorization for signing for legal persons (see [Sonntag 2000]).

6 Conclusions

We have taken a look on who has to take responsibility for actions of an agent and found that the differentiation

between the owner of the agent (who provides its parameters) and the creator of the code is a difficult one. The requirements for the owner of a public server for agents are rather moderate and finally defined in law: Only if he receives knowledge about illegal actions or content he must take action.

Defining electronic communication as obligatory between companies and consumers is not possible through electronic means; offline negotiation must take place in advance. This however is no problem if the consumer initiates communication. With agents the acceptance to receive messages in this way can be presumed if a common standard (e. g. defined in the agent system) is used.

With a technically relatively simple method a server can prove that he supplied an agent with some information. Since this requires storing a lot of data the method will be useable only for larger companies.

In the EU agents cannot create legally binding digital signatures, but their signature can be used as evidence. The main problem will be to prove that no interference with the agent took place. This can be partially achieved by a hand-off. The host must have caused states, which cannot be reached with the given input from the initial state (as evidenced by the signature of the server on receiving the agent).

A lot of legal issues in the context of components and agents (especially mobile ones) as a special form of them are still unsolved. For agents to take on a larger role in E-Commerce these need to be solved. The main focus should be put on creating evidence, as with this present, legal proceedings will often be unnecessary. This is very important because mobile agents are very likely to be active in different countries which might cause many problems of jurisdiction otherwise.

Acknowledgments

This paper is a result of a project sponsored by the Country of Upper-Austria (Wi/Ge 201.515/1-2000/Wwin).

References

[Aglets] IBM Aglets Software Development Kit Home http://www.trl.ibm.co.jp/aglets/ (28.9.2001)

[ECD] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), ABl. 17.7.2000 L 178/1

[ECL-Draft] Ministerial Draft for the E-Commerce Law: Ministerialentwurf betreffend ein Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz - ECG)

[FIPA] FIPA ACL Specifications http://www.fipa.org/repository/aclspecs.html (28.9.2001)

[KIF] UMBC KIF Web http://www.cs.umbc.edu/kse/kif/ (28.09.2001)

[Koziol/Welser 2001] Welser, R.: Grundriß des bürgerlichen Rechts. Von Helmut Koziol und Rudolf Welser. Band II Schuldrecht Allgemeiner Teil, Schuldrecht Besonderer Teil, Erbrecht. 12 Auflage. Wien: Manz 2001

[KQML] UMBC KQML Web http://www.cs.umbc.edu/kqml/ (28.9.2001)

[POND] Agent System POND: http://www.fim.uni-linz.ac.at/Research/Agenten/index.htm (28.9.2001)

[SigD] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, ABl. 19.1.2000 L 13/12

[SigL] Austrian Federal Electronic Signature Law: Bundesegesetz über elektronische Signaturen (Signaturgesetz- SigG), BGBl I 190/1999

[SigO] Austrian Signature Order SigV: Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung - SigV) vom 2.2.2000. BGBl II 30/2000

[Sonntag 2000] Sonntag, M.: Electronic Signatures for Legal Persons. In: Hofer S., Beneder, M. (Ed.): IDIMT'00. 8th Interdisciplinary Information Management Talks. Linz: Universitätsverlag Rudolf Trauner 2000, 233-256

[USElSigAct] Electronic Signatures in Global and National Commerce Act http://www.dud.de/dud/documents/usesignact0608.pdf (28.9.2001)

[Vigna 1998] Vigna, G.: Cryptographic Traces for Mobile Agents. In: Vigna, G. (Ed.): Mobile Agents and Security. Berlin: Springer 1998 (LNCS 1419)

[Zankl 2001] Zankl, W.: Rechtsqualität und Zugang von Erklärungen im Internet. ecolex 2001, 344