Journal of Information, Law and Technology

No Remedy for Disappointed Trust - The Liability Regime for Certification Authorities Towards Third Parties Outwith the EC Directive in England and Germany Compared

Steffen Hindelang
LLM, Sheffield
St.Hi@gmx.de

This is a **refereed** article published on: 22 March 2002

Citation: Hindelang S, 'No Remedy for Disappointed Trust - The Liability Regime for Certification Authorities Towards Third Parties Outwith the EC Directive in England and Germany Compared', Refereed article, *The Journal of Information, Law and Technology (JILT),* 2002 (1). <http://elj.warwick.ac.uk/jilt/02-1/hindelang.html>

Abstract

In history the seal was replaced by the hand written signature. With the dawn of the digital age the days of the hand written signature are now also numbered. Fairly soon electronic data communication will render paper superfluous, and hand written signatures will be replaced by their ‘unequal sisters’ - the electronic signature, also called digital signature.

This paper will look at one of the legal aspects uniquely connected with electronic signatures - the liability of certification authorities (CA). Since our new signatures will consist only of a binary code somebody must link this code with our identity. This function is performed by CAs, stating both the identity and binary code in one electronic document called certificate. The question of liability arises when, intentionally or negligently, a binary code is linked to a non-corresponding identity. This study does not deal with the legal relation between CA and certificate holder, but with the largely unsolved, or not sufficiently solved, problems of professional liability for the provision of information towards third parties. In other words, this paper focuses on the liability regime which applies between a CA, and a third party who uses the certificate to validate the identity of a certificate holder intending to transact with the third party.

The European Union has introduced minimum liability rules for a group of certificates which are supposed to have a very high security standard, thus potentially increasing the confidence of the third party regarding the certificate. We will, however, learn that the vast majority of certificates are governed solely by national liability rules. So far the elaboration of these liability regimes have been largely neglected and underestimated by academic writers in England and Germany. Due to its practical significance, an urgent explanation and elaboration is thus needed. The concern of this paper will, therefore, be to explore the liability regimes for certificates outside the scope of the EU regulations.

The first section deals with the comprehension of technology and usage of electronic signatures, which is a necessary prerequisite. The second section will provide an introduction to the issue of liability. It in order to distinguish the liability regimes applicable to different categories of certificates in the EU, this section will also briefly outline the legal framework created by the EC Directive. The third section will initially identify relevant English liability rules before exploring whether such rules are suitable and sufficient to cover the special liability situation in which a CA and a relying party may find themselves. The same process of exploration and evaluation will be applied to the German liability rules in the fourth section. The fifth section will compare the results produced by such an exploration and evaluation of the English and German system.

The paper reaches the following initial conclusions: there are many (perhaps too many) minor and major obstacles in both German and English law which question the success of any claim by a relying party. A strong liability regime (which would particularly enhance confidence in ‘non-qualified’ certificates, and generally in electronic communication and commerce) is practically not in existence! If the present laws are applied, the question of whether to boost e-commerce through consumer confidence or through low legal obstacles for businesses operating in the respective market seems to be decided in clear favour of the latter one. It is doubtful whether this decision was intended, since relying parties could be deprived of any legal protection.

This paper is, therefore, convinced of the need to find a balance between both conflicting interests, since somebody who takes up trust, as a CA does, must prove reliability (also) through liability. On the other hand, however, businesses must be enabled to protect themselves against the risk of liability in an indeterminate amount to an indeterminate group.

Since the existing laws in both countries contain many uncertainties and obstacles, (making a success of a relying party's claim unlikely) this paper suggests the introduction of a special tortuous liability rule, which eliminate the two main obstacles for a successful claim:

the burden of proof imposed upon the relying party; and

the threat of liability in an indeterminate amount, to an indeterminate class, which is owed to the open character of the Internet.

To deal with the first obstacle it may be sufficient to reverse the burden of proof. The CA is in a (much) better position to prove that it has not acted negligently, since it is familiar with technology and its own organisational structure. In order to tackle the second obstacle, two equally important measures may be suggested. On the one hand, there might be introduced a new statutory tort, subjecting the CA to liability for non-qualified certificates similar to the EC Directive. The courts would no longer be troubled by the notion of liability in an indeterminate amount, to an indeterminate class while establishing a duty of care (England), or a protective effect of the certification contract towards relying parties (Germany), since liability is imposed by statute. This, however, would solve the legal, but not the factual problem of liability in an indeterminate amount, to an indeterminate class. Therefore, to enable businesses to manage effectively the enormous liability risk one may expressly permit by statute exemption and limitation clauses which intend to limit the liability to a certain amount per annum and/or per series of incidences, coupled with a minimum amount of liability, which would cover ordinary incidences and would prevent abuse of these exemption clauses.

A call for harmonisation (on an European level) might be premature, since one must first consider the other jurisdictions within Europe.

The author is aware of the fact that he can only offer a first glance on the whole topic, due to the scope of the paper and the unexplored nature of the issue.

Keywords: Digital Signature, Liability, Certification Authority, Electronic Certificate, Relying Third Party, Certificate Holder, Germany, England, European Community, Comparison, E-commerce, E-business, Trust, Confidence.

1. Introduction

In history, the seal was replaced by the hand written signature. With the dawn of the digital age, the days of the hand written signature are now also numbered. Fairly soon electronic data communication will render paper superfluous, and hand written signatures will be replaced by their ‘unequal sisters’ - the electronic signature, also called digital signature. The first harbingers of the new technology have already arrived. In 1999 Finland introduced the digital Identification Card equipped, of course, with an electronic signature and in electronic commerce the electronic signature has begun to challenge the widely used credit cards. In the near future electronic signatures will play a most significant role in our every day life.

This paper will look at one of the legal aspects uniquely connected with electronic signatures - the liability of certification authorities (CA). Since our new signatures will consist only of a binary code, somebody must link this code with our identity. This function is performed by CAs, stating both the identity and binary code in one electronic document called a certificate. The question of liability arises when, intentionally or negligently, a binary code is linked to a non-corresponding identity. This dissertation does not deal with the legal relation between CA and certificate holder, but with the largely unsolved, or insufficiently solved, problems of professional liability for the provision of information towards third parties. In other words, this paper focuses on the liability regime which applies between a CA, and a third party who uses the certificate to validate the identity of a certificate holder intending to transact with the third party.

The European Union has introduced minimum liability rules for a group of certificates which are supposed to have a very high security standard, thus potentially increasing the confidence of the third party regarding the certificate. We will, however, learn that the vast majority of certificates are governed solely by national liability rules. So far, the elaboration of these liability regimes have been largely neglected and underestimated by academic writers in England and Germany. Due to its practical significance, an urgent explanation and elaboration is thus needed. The concern of this paper will, therefore, be to explore the liability regimes for certificates **outside** the scope of the EU regulations.

Before commencing into legal territory, the first chapter deals with the comprehension of technology and usage of electronic signatures, which is a necessary prerequisite. The second chapter will provide an introduction to the issue of liability. It in order to distinguish the liability regimes applicable to different categories of certificates in the EU, this chapter will also briefly outline the legal framework created by the EC Directive. The third chapter will initially identify relevant English liability rules before exploring whether such rules are suitable and sufficient to cover the special liability situation in which a CA and a relying party may find themselves. The same process of exploration and evaluation will be applied to the German liability rules in the fourth chapter. The fifth chapter will compare the results produced by such an exploration and evaluation of the English and German system. Comparison is only used here as a method to offer an initial explanation of whether, and why, a claim against a CA might be more likely to succeed in the courts of one or the other jurisdiction. The results gained from this exercise and the previous chapters will enable us to judge whether, and for whom, the existing liability regime may be seen as an additional source of confidence in electronic signatures technology. Confidence is necessary to boost the growth of secure electronic communication and commerce. Ultimately, we have to decide whether to suggest an additional liability rule.

The author is aware of the fact that he can only offer a first glance on the whole topic, due to the scope of the paper and the unexplored nature of the issue. Any critique and comments derived from this study are, therefore, very welcomed.

2. Technology and Usage

We have witnessed the rapid development of the Internet and multimedia sector in recent years. Paperless communication, based on electronic documents such as Emails, has become one of its most significant features.

Paperless communication contains enormous advantages. Documents are created and processed within the same medium. Paper is no longer necessary. The bodiless documents can be mailed around the world almost without any loss of time; they are available for numberless users in the original at the same time; they do not need much storage and archive space. However, unfortunately also specific disadvantages are connected with this kind of communication. The two most troublesome are mentioned as follows:

(1) manipulation is hardly detectable or provable;

(2) the identity of the sender is difficult to establish (Roßnagel, 1998).

The development of a technique which can ensure the authenticity and integrity of electronic documents has become necessary to overcome these drawbacks. Scientists created a technology which is known as electronic signature. This technology is widely based on public key cryptography. Electronic signatures accompanied by an electronic certificate ‘can provide three important functions:

(1) **Authentication** - to authenticate the identity of the person who signed the data so it is known who participated in the transaction.

(2) **Integrity** - to protect the integrity of data so it is possible to know the message read has not been changed, either accidentally or maliciously.

(3) **Non-repudiation** - to allow it to be proved later who participated in a transaction so that it cannot be denied who sent or received the data’(Angel, 1999).

2.1 Technology

No attempt will be made here to explain the rather complex underlying technology in any detail. Readers who are unfamiliar with cryptographic terminology and techniques should consult, in addition to what is stated here, the many excellent sources available which can provide the relevant technical background (see for example, Reed, 2000, ABA, 1996). The importance of understanding the technology cannot be overstated. In order to facilitate the reconstruction of the technological operations the reader might be advised to make use of the appendices and glossary at the end of this dissertation.

2.1.1 What is 'Public Key Cryptography'?

Public key encryption uses two different but mathematically related keys, each of which will decrypt documents encrypted by the other key. One key, chosen arbitrarily, is used to transform data into a seemingly unintelligible form and is kept secret, while the other is made public. All effective electronic signatures require the use of a 'one-way function' (irreversibility). This means that if a document, signed electronically by Alice with her private key, is sent to Bob, Bob must be able to decrypt the document's signature element with the help of Alice's public key, but must not be able to re-encrypt it with this key (Reed, 2000a). In other words it must be 'computationally infeasible' to derive the private key from the knowledge of the public key. Otherwise the discovered private key could be used to forge digital signatures of the holder (ABA, 1996).

2.1.2 How Does the 'Public Key Cryptography' Process Work?

Alice wants to send a word document to Bob(See Figure 1: Sending an Electronically Signed Document).

1. Alice passes the document through an algorithm, called a *'digest' or 'hash' function*. This function carries out a mathematical operation on the original document. It creates a unique and concise version of the original text - the *'message digest'*.

2. Alice then encrypts the message digest with her *private key*. Encryption is carried out by performing a series of mathematical functions (an encryption algorithm) which has two inputs: the 'message digest' which is nothing more than a string of 1s and 0s and the private key which is itself also a number. The result of this operation is a series of different numbers, which (in a technical sense) form the actual *electronic signature* (Reed, 2000a).

3. Alice sends the plain word document and her electronic signature to Bob.

4. When Bob receives the message, his computer and software perform mathematical operations in order to determine whether the document was altered in transit (**Integrity** of the document) and whether Alice's public and private key correspond (See Figure 2: Validating an Electronically Signed Document).

5. Bob's system takes Alice's digital signature, and uses her *public ke*y to decrypt the digital signature. This operation will (re-)produce the 'message digest' of the document Alice **sent**. If a private key other than the one corresponding to the public key of Alice was used to encrypt the sent

message digest, the electronic signature will not be verified.

6. At the same time the plain document Bob received is run through the same hash function (!) that Alice used. This will provide Bob with the message digest of the document he **received**.

7. Bob will then compare the two message digests. Any change in the word document while in transit, no matter how slight, would lead to a significant change of the message digest generated out of the received word document when the same hash function is used. Each document has its unique message digest. However, if the message digest produced from the electronic signature and the message digest produced from the plain document received are the same, Bob will know that the document he received, had not been altered in transit. Alice's signature has been validated.

2.2.3 Certification Infrastructure (see Figure 4: Certification Structure).

Certification Authorities

However, the utility of an electronic signature as an **authenticating tool** is limited by the ability of the recipient to ensure the authenticity of the key used to verify the message digest. In other words, it proves only that private key and public key belong together. If the evil Dr. No is forging a message from Alice he will send his own public key as well, claiming that it actually belongs to Alice. In order to rely on the authenticity of that public key, however, Bob needs to get it from some source other than Alice. If Bob has access to Alice's public key from some outside source, and uses it to verify the message signed with Dr. No's private key, purporting to be Alice, the verification will fail, revealing the forgery.

In a nutshell, if Alice and Bob had no previous dealings, are strangers, then no electronic signature will reliably identify them to each other without assistance of some outside source to provide a link between their identities and their public keys. Any outside source that reasonably inspires trust will suffice. Here certification authorities (CA) come in.

A *certification authority* is a body, either public or private, that seeks to fill the need for trusted third party services in electronic commerce by issuing electronic certificates, signed electronically, that attest to some fact about the subject of the certificate (Froomkin, 1996). In order to be willing to accept certificates issued by a CA 1 the recipient of this certificate, in our case Bob, must have confidence that the CA 1's public key is really the CA 1's and not another manifestation of the wily Dr. No. One way to achieve this confidence is to have an identifying certificate from another CA (CA 2), certifying CA 1's key. The public key of CA 2 might be certified by a CA 3 and so on. Ultimately, this will lead to a *certificate chain*, with a root certificate at the bottom of the tree. However, this just shifts the problem to the validity of the last CA's public key. One solution to this problem is to establish a governmental root CA, which usually inspires trust. Another solution is to establish a business self-regulatory body monitored by governmental authorities.

Certificates

A *certificate* is a digitally signed statement by a CA that provides independent confirmation of an attribute claimed by a person proffering a digital signature. In technical words, a certificate is a computer based record which:

(1) identifies the CA issuing it,

(2) names, identifies, or describes an attribute of the subscriber (e.g; a subject's name, where a subject resides, the subject's age, a subject's membership in an organisation)

(3) contains the subscriber's public key, and

(4) is digitally signed by the issuing CA (Froomkin, 1996).

Usually it also contains information about the level of inquiry used to confirm the fact. Since personal circumstances change and the reality represented by the certificate is out of date, certificates have limited periods of validity or are subject to periodic re-confirmation by the CA. Certificates which are outdated or have been compromised, e. g. by disclosing the private key, are listed in so-called *certificate revocation list* (CRL), which is maintained by the issuing CA.

Recalling our example given above, if Alice wants Bob to enter into dealings with her, she will not only send the plain word document and her electronic signature but will also ensure that Bob has access to her certificate, which links her electronic signature, or more precisely her public key, to her identity. Alice's certificate might be sent by Alice (most common situation), or posted on a web page of her CA or it could also be e-mailed by Alice's CA to Bob. In some cases, the choice might affect the legal regime that applies to the CA.

2.2 Usage

That electronic signature is not only a beloved toy of some avant-garde scientists but a practical tool facilitating the continued growth of the Internet and multimedia society, which can be witnessed by the following examples. By December 1999, Finland was the first country on earth to introduce the digital ID card. The so-called 'Finn-Oath', a smart card with a microchip, allows a person to register a new permanent residence via the Internet from home or at publicly accessible terminals which look like cash-dispensers. New applications are currently on the way or in a test phase in order to create a real multifunctional card out of the 'Finn-Oath'. Alternative functions might include: public library card, tax declaration, secure Email communication, Home-banking, access to company computer networks and secure contracting and payment via the Internet without the need of a credit card. To ensure integrity and authenticity of the data, all operations are signed electronically with the private key already stored in the card. The electronic signature is protected against misuse or abuse by a PIN. Without an electronic signature many of the above mentioned features would not be possible, because of a lack of trustworthiness and/or legally binding character (Gründel, 2000).

On the 1st January 2000 the European Union started the project FASME (Facilitating Administrative Service for Mobile Europeans <http://www.fasme.org/fasme/english/index_e.htm>). The aim is to facilitate administrative processes in Europe connected with a change of residence and work within Europe, e. g. police registration, registration of cars, changes in social insurance and tax liabilities. The functionality of the FASME card will later be extended to private sector applications. Again, integrity and authenticity of data is backed up by an electronic signature (Gründel, 2000).

E-government (eg; The Economist, 2000, Der Spiegel Online, 2000, and Uwer, 2000) is one area of application. However, the application in the private sector will be more important by far.

> 'Security remains the biggest worry for businesses and consumers engaged in online transactions and, according to many experts, it is the biggest single obstacle to the further growth of e-commerce. Whether it is the risk of fraud, of vital communications going astray or credit-card details being stolen, many companies and individuals regard trading over the Internet with some trepidation' (Dawe, 2001).

The need for more e-businesses to use electronic signatures is paramount. The wide application of the electronic signature technology will make business happier about accepting orders totalling hundreds of thousands of £ over the Internet, and may persuade online banks to allow their customers to freely transfer funds to any other account, without having to write cheques. Consumers will benefit directly from the increased trust, businesses and governments will have in them, if they can conclusively prove their identity and create a binding instruction which they cannot later deny (Dawe, 2001). Annoying and insecure detours as e. g. the provision of credit card details, as well as uncertainties about the business behind the web site, will belong to the past (Der Spiegel Online, 2000).

3. The Liability Issue and the Future European Legal Framework on Electronic Signatures

3.1 The Liability Issue

Certification authorities are dependent on the ability of their certificates to inspire trust in the reliability of the information contained. Trust may be gained first and foremost from innumerable secure and successful communications in which certificates of a certain CA have proved to be reliable and trustworthy. Business activities of a CA in the non-digital world, such as postal services or banking activities, may also contribute to an enhancement of confidence people have in certificates supplied by these institutions.

But what will be the situation if the certificate proved to be unreliable as a result of the

CA’s failure? There are many reasons why a certificate might be unreliable.

‘The most obvious of which are:

> *- the CA fails to take proper evidence of the holder’s identity;*
>
> *- the encryption technology used to link that identity with the holder’s public key and the CA’s public key is weak, allowing ‘forged’ certificates to be produced;*
>
> *- the CA does not keep proper records, so that revocations are not recorded or the identification process cannot be proved in court; or*
>
> *- the CA employs incompetent or dishonest staff, thereby compromising the reliability of the information in the certificate’* (Reed, 2000a).

Thus, electronic signatures accompanied by a certificate might not be so trustworthy as certain groups want us to believe. Here liability rules could make a crucial contribution to enhance confidence in certificates in particular, and signature technology in general. In the case of disappointment in the confidence as a result of a failure of the CA, the awareness of the relying party that he can recover the loss which he suffered out of his reliance on the certificate might prove to be one of the strongest ‘crowd pullers’ for trustworthy electronic communication and, eventually, electronic commerce. How strong this ‘crowd puller’ will be depends on the applicable liability rules.

3.2 The EC Directive 1999/93/EC - Different Rules for Different Certificates

The legal framework for the liability of CAs towards third parties as it has stood since the 19th January 2000, was created by the *Directive 1999/93/EC on a Community framework for electronic signatures* (ESD). Depending on what kind of certificate was relied on, two different liability regimes will apply. For one kind of certificates, liability of the issuing CA towards third parties has been harmonised by imposing minimum standards. All other certificates will continue to be governed by (national) general liability rules as they stand now. Before turning towards the two different liability regimes and how to distinguish them, it might be desirable to glance at the Directive as a whole in order to comprehend the legal environment which has been created by it.

3.2.1 The European Legal Framework on Electronic Signatures in General

The Directive was issued after the adoption of some national laws, regulating electronic signatures, which did not share very much in common. For example the German Digital Signature Act 1997 provided for a mandatory accreditation scheme coupled with high security standards for certification service providers (see further Rebel and Koenig, 1999). In contrast, the prevailing notion in England has been that of business self-regulation.

The Directive, therefore, aims to prevent divergent rules with respect to legal recognition of electronic signatures and the accreditation of *certification-service-providers* in the Member States, which may create a significant barrier to the use of electronic communications and electronic commerce. Furthermore, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies (ESD, recital (4)). Moreover, the ESD contains also a liability provision. Considering that all member states have to comply with the Directive, it is reasonable to expect that the entire EU will have a twofold digital signature system (Sinisi, 2001). There will be, on the one hand, an *advanced electronic signature* that will have the same value as a hand written signature and be admissible as evidence in legal proceedings (ESD, Art. 5 (1)). On the other hand there will be a 'regular' *electronic signature* which may, at least, not be denied legal effectiveness and admissibility as evidence on the grounds that it is in electronic form, or not based upon a qualified certificate, or not based upon a qualified certificate issued by an accredited certification-service-provider, or not created by a secure signature-creation device (ESD, Art. 5 (2)). An advanced electronic signature is based on a *qualified certificate* and is created by a *secure signature creation device*· (ESD, Art. 2 (10)). In addition, in Art. 3 (2), the EC Directive provides for the introduction of a **voluntary** accreditation scheme for certification-service-providers, here just mentioned for the sake of completeness. Accreditation is based on an enhanced level of certification-service provision. If implemented in national law, certificates issued by these certification-service providers are most likely be used in the public sector, where additional requirements for the recognition of electronic signatures are permissible under Art. 3 (7) ESD.

3.2.2 The Liability Provisions

Having outlined the basic features of the EC Directive in short, we turn now our attention towards the specific issue of this paper: the liability of certification-service-providers towards third parties and its treatment in the Directive. While in general certification-service-providers providing certification-services to the public are subject to national rules regarding liability (ESD, recital (22)), a **minimum standard of liability** towards third parties is introduced **for qualified certificates**. The relying party's confidence, which is 'artificially' enhanced in the Directive by the promise of high standards which must be met in order to issue and obtain such a qualified certificate, is backed up by a EU wide standard of minimum liability of certification-service-providers. This is for certain cases in which the certificate might be unreliable as a result of the CA's failure. The text of Arts. 6 (1) and (2) of the Directive runs as follows:

> *'1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:*
>
> *(a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;*

> *(b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;*
>
> *(c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;*
>
> *unless the certification-service-provider proves that he has not acted negligently.*
>
> *2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.'*

The certification-service-providers have the possibility to indicate limitations on the use and value of transaction of the certificate, which enables them to manage their risks more effectively. Arts. 6 (3) and (4) state the following:

> *'3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate, provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.*
>
> *4. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties.*
>
> *The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded'.*

Section (1) to (4) of Art. 6 , however, are without prejudice to EC Directive 1993/13/EEC of 5th April 1993 on unfair terms in consumer contracts.

To sum up what was outlined above, the applicable set of liability rules is dependent on the type of certificate. There is the liability regime for **qualified certificates**, which will be more or less the same across Europe after the implementation of the EC Directive. It is unlikely that member states will introduce a significantly higher standard than suggested by the Directive, since it would put a CA situated in the respective state at a competitive disadvantage. However, **all other certificates** ('non-qualified certificates'), which do not meet the requirements for qualified certificates, are subject to the general liability rules as they stand now! Qualified certificates will not be, at least in the foreseeable future, a mass product. Due to their high security standard they are too cost-intensive for every day life. In contrast, non-qualified certificates are cheaper. Their security standard is flexible and their content can be customer-tailored. These will certainly play a major role in every day electronic communication and commerce, which do not require the high standard of security that only a qualified certificate may be able to offer. **It must be stated once again that this paper only focuses on the comparison of liability regimes for the latter category - the category of 'non-qualified' certificates!** For the sake of clarity, however, the following section will give a brief overview over the state of implementation in Germany and England.

3.2.3 Implementation

Germany has already implemented the EC Directive in the Act for a Basic Framework for Electronic Signatures 2001 (Signature Act (SigG)) (*'Gesetz über Rahmenbedingungen für elektronische Signaturen'*) and respective Ordinance. § 11 (1) *SigG* imposes liability towards third parties on a certification-service-provider if he:

> *'...infringes the requirements under this Law and the statutory ordinance under [§] 24, or if his products for qualified electronic signatures or other technical security facilities fail, he shall reimburse a third party for any damage suffered from relying on the data in a qualified certificate or a qualified time stamp or on information given in accordance with [§] 5(1). Damages shall not be payable if the third party knew, or must have known, that the data was faulty.'*

§ 11 (1) is subject to the subsections (2) to (4). Furthermore, the

> '...certification-service-provider shall be obliged to make appropriate cover provisions to ensure that he can meet his statutory obligations for reimbursement of damages...'

The liability for 'non-qualified' certificates is also left to the existing law. In §§ 15 and 16 the German legislator enacted a voluntary accreditation scheme, as already described above.

The United Kingdom has not yet suitably implemented the Directive. The consultation on the EC Directive closed on the 19 June 2001 (DTI, 2001a). A summary of the responses has yet been published and can be accessed on the UK Department of Trade and Industry (DTI) website (DTI, 2001b). The liability issue is addressed under 'Question 6' of the DTI document. So far, only Art. 7 (2) of the Directive has been implemented via the Electronic Communications Act 2000. During the elaboration of the present liability regime in England occasional digression will be made to outline the areas of law which need to be adjusted in order to comply with EC law.

We shall now proceed with the discussion of the English liability regime in Chapter 3, before turning to the German liability regime in Chapter 4.

4. The Present Liability Regime in England

4.1 Contractual Liability

One possibility to recover the loss caused by reliance on an incorrect certificate would be to construe a contract, which would warrant the accuracy of the certificate in some way, between the CA and the relying party. The inaccuracy of the information would amount to a breach of contract and would allow the relying party to treat his own contractual performance obligations as being at an end and to claim damages. Another way might be to imply a contract for the benefit of a third party, more precisely, a contract between the CA and the certificate holder for the benefit of the recipient of the electronically signed document, the relying party. Due to the different parties to the contract, the two possibilities are discussed separately.

4.1.1 Contractual Relation CA - Relying Third Party

Offer and Acceptance

One essential requirement for the formation of a contract is the offer and its acceptance (Treitel, 1999). Two alternatives for the construction of the offer and its acceptance have been suggested:

> (a) The relying party makes an offer '...to rely on the certificate if in return the CA made promises about the accuracy of the information in the certificate. The CA's response that a certificate was still valid would be the acceptance' (Reed, 2000a).
>
> (b) 'The CA had made a unilateral offer to the whole world, along the lines of the case *Carlill v. Carbolic Smoke Ball Co.*, promising certain things to any person who accepted its offer by undertaking the conduct required by the offer - in this case, by relying on the certificate' (Reed, 2000a).

Alternative (a)

Alternative (a) would require **direct** communication between the CA and the relying party from which an offer and acceptance can be extracted, because a person cannot claim to have accepted an offer of which he was unaware (Treitel, 1999). At times, this constitutes a difficulty. In practice, the relying party, Bob, will have received the certificate and public key from the sender of the message, Alice. Thus, if Bob has confidence in Alice's certificate there will be no contact between Bob and Alice's CA, since Bob has received all information necessary to validate the signature of Alice (Figure 3: Validating an Electronically Signed Document with Certificate).

However, even if one might be able to imply an offer and acceptance from a communication which occurs when, for example, the relying party is suspicious about the validity of the certificate and interrogates the CA's Certificate Revocation List (Reed, 2000a), or the relying party obtains Alice's certificate and public key from the CA's web site, uncertainty might arise when one turns one's attention to another fundamental element in the formation of a valid contract in English law: the element of consideration.

> ‘A valuable consideration, in the sense of law, may consist either in some right, interest, profit or benefit accruing to one party, or some forbearance, detriment, loss or responsibility given, suffered or undertaken by the other’.

It is not entirely clear whether the promise ‘to rely on the certificate’ is sufficient to amount to a consideration. What will be the economic valuable benefit which the CA will gain or the economic valuable loss which the relying party will suffer when the latter promises ‘to rely on the certificate’? Surely, in our case the promise amounts to more than a sentimental motive or natural affection for promising. However, the relying party does not lose anything with the promise. His commercial freedom is in no way limited, therefore no loss is suffered merely by giving the promise to rely upon the certificate. On the other hand, one may argue that a valuable benefit for the CA could be seen in a general enhancement of the market for ID certificates. As more people trust these certificates and their issuing CAs, this technique may be used more frequently. The demand for certificates might increase. In particular, that the relying party has confidence in the certificate, and thus does not undertake his own inquiries about the identity or other attributes of the certificate holder, just enables the CA to run its business. One may conclude that the CA will gain a benefit from its promise to provide accurate information.

Alternative (b)

Turning now to the second alternative - the offer to the whole world - the question of whether the relying party has any view about the CA’s intention to make an offer arises. If the relying party does not enter into direct communications with the CA it may not be obvious for the relying party, at least as long as the electronic signature technology has not become everyday business, that the CA ‘wants’ to form a legally binding contract. While one may argue that the Internet presentation of the CA constitutes a form of conduct which induces a reasonable person to believe that the CA intends to be bound, even though in fact the CA may not have such an intention, it is doubtful whether the state of mind of the relying party - not having formed any view about the CA’s intention - is sufficient to bind the offeror. This situation has given rise to a conflict of judicial opinion. One view demands that the offeree actually held that belief. For the opposing view, it is sufficient that the offeree does not actually know that the offeror does not have any such intention. It remains to be seen which opinion will be followed by the courts.

Terms of Contract

Even where the courts are able to construe a contract much uncertainty will remain as to the terms of that contract (Reed, 2000a). Certainly, the CA makes some promise about the accuracy of the information contained in the certificate. But what exactly is the content of the contractual duty owed by the CA and which liability does it accept? (Reed, 2000a).

Precise Content of the Contractual Duty

In establishing the precise content of the promise two possibilities may be distinguished:

> (1) The CA is warranting that the information is accurate, and thus accepting **strict liability** or

> (2) the CA is '...warranting no more than it took **reasonable care** to ascertain the accuracy of the information, so that liability will only arise if the relying party can prove a failure in that respect' (Reed, 2000a, 139).

It has been said that:

> 'where the contract is one for the supply of *services alone*, liability is often based on fault. Thus the general rule is that contracts under which services are rendered by professional persons impose duties of care only'.

It is indeed not obvious whether the CA supplies a service or a good. However, it seems to be plausible to consider the supply of accurate information as a service because a:

> 'certificate resembles a professional's opinion in that a certificate ordinarily is the tangible memorial of a process of analysis in which the subject's credentials were checked in some manner' (Froomkin, 1996, III. A.1).

Furthermore, some guidance may be also offered by the *EC Directive on a Community framework for electronic signatures*. If the Directive suggests that the liability for incorrect qualified certificates (ESD, Art. 2 Nr. 10) should be based on a proof of a failure (ESD, Art. 6 (1), (2)), then it would be illogical to impose a stricter liability upon a CA which offers a less reliable certificate (*argumentum a maiori ad minus*). Thus, it seems reasonable to follow the general rule that only reasonable care is owed in the case of 'non-qualified' certificates.

Having established that only reasonable care is owed in ascertaining the accuracy of the information in the certificate, one must now answer the question of which level of accuracy is owed. This is the issue of the scope of the contractual duty. Since this is a case of dealing with implied contractual terms the courts should be able to take into account any custom and practice in the field of CA activity. CAs 'tend' to publish so-called *Relying Third Party Charters* and *Certification Practice Statements (CPS)* which define the representations they make and warranties they hold out in respect of certificates. If a CA took all reasonable steps and complied with all the quality control procedures which it had laid down for itself, loss caused by an inevitable failure to link a public key accurately with a person will not be recoverable since no breach of contract has occurred. Thus, the scope of the contractual duty to be expected can be manipulated by notices properly drawn to the attention of the relying party (Harrison, 2000). This is, however, subject to the Unfair Contract Terms Act 1977 and the Unfair Terms in Consumer Contracts Regulations 1994.

Scope of Liability - Value of the Claim

General Considerations

CAs try not only to manipulate their primary contractual duties, but attempt to exclude and/or limit their liability in the event of a breach of these duties. In general, in the event of a breach of contract, the plaintiff can treat his own contractual performance obligations (to have confidence in the certificate) as being at an end and may sue for damages.

Damages awarded intend to put the plaintiff in the position he would have been in, had the contract been performed, subject to the rules of factual causation, remoteness of damages and mitigation of loss (Oughton and Lowry, 2000, 136). The remoteness of damages deserves in our case a closer look. It was held that a distinction must be drawn between normal and abnormal loss. Normal loss is loss which arises naturally in the usual course of events from the defendant's breach of contract.

The courts require a high standard of foresight by the defendant. The question to be asked therefore is whether the defendant realised that it was reasonably certain that the harm suffered by the plaintiff might result from the breach. What might be understood as 'reasonably certain' in the case of a CA is difficult to anticipate. However, one might argue that the courts would probably adopt a narrow approach in order to allow a CA to deal with the enormous financial risks involved in its business. In theory, even a certificate with a minimal 'permitted' transaction value of - let's say £ 10 - can cause damage worth millions of Pounds in no time if only enough people rely on it and suffer loss, thereby taking into account that hundreds of thousands of signatures can be generated in a few seconds. However, underlying policy interests may play a certain role. If the court is of the opinion that confidence in the new technology, in particular of consumers, it best promoted by a strong liability regime, damages awarded might be significantly higher. What is necessary is to reach a 'healthy' balance between business interests and general policy arguments.

Exemption and Limitation Clauses

CAs will, naturally, try to exclude and/or limit their liability in advance in order to minimise economic and legal uncertainties. Two forms of exemption/limitation clauses are commonly found in practice. Firstly, references to other documents contained in the certificate are very commonly, as e.g; so-called Trusted Third Party Charters, CPSs and notices posted on the web sites of the CAs. These documents usually limit the liability to a certain amount per incident, per series of incidences and per annum, and in addition, exclude:

> '...direct or indirect loss of profits, business or anticipated savings and indirect or consequential loss or damage or for any destruction of data' (BT, 2000b).

A second (special) category of disclaimers are notices included in certificates which state maximum limits of the value of transaction or they limit the purposes of usage of a certificate. The legal nature of this category of legal declaims is ambiguous.

In the following sub-sections the legal effects and the lawfulness of the above mentioned clauses will be discussed.

Clauses Which Exclude and/or Limit the Liability in the Event of a Breach of a Contractual Duty

The BT TrustWise Relying Third Party Charter may serve as an example for the category of legal disclaimers which partly exclude and partly limit the liability in the event of a breach of a contractual duty. It states the following:

> *'BT's liability to you is limited to £250,000 for any one incident or series of related incidents and to £500,000 for all incidents in any period of 12 months. BT is not liable to you (including for negligence) for direct or indirect loss of profits, business or anticipated savings, nor for any indirect or consequential loss or damage or for any destruction of data. BT accepts unlimited liability for death or personal injury resulting from its negligence and the limits set out above do not apply to such liability. BT is not liable to you for the acts or omissions of other providers of telecommunications or Internet services (including domain name registration authorities) or for faults in or failures of their equipment'*(BT, 2000b).

Under Law of England and Wales such statements are subject to the Uniform Contract Terms Act 1977 (UCTA) and the Unfair Terms in Consumer Contracts Regulations 1994.

S. 3 (1) in connection with 3 (2) (a) of the UCTA 1977 provide that the *proferens* (=CA) cannot exclude and/or restrict liability in respect of its own breach of contract, unless to do so satisfies the test of reasonableness. What might be reasonable depends on the facts of the case, which (particularly in relation to the new technology) is difficult to predict. However, where the notice purports to limit the liability to a specified sum, as it is the case in the given example, s.11 (4) of the UCTA 1977 provides an express rule that the court should have particular regard to the insurance position by considering whether insurance was available to the *proferens* and whether he had sufficient resources to meet liability. Some general guidelines have also been judicially indicated and might be of value for our purposes. Not only in cases where the notice purports to limit the liability to a specified sum, but also in all other cases of exemption and limitation the courts have openly considered **which of the parties could have best insured itself against the risk of the loss** under consideration.So far as the author is aware, there has yet been no insurance made available to relying parties, which would cover the loss suffered from an incorrect certificate. A CA might be in a better position to insure the risk connected with a unreliable certificate. However, coverage problems might arise, e. g. when an unreliable certificate causes multiple losses to different people. The maximum coverage can quickly be exceeded. CAs have tried to deal with the problem of obtaining suitable insurance coverage, on the one hand, by limiting the liability to a certain amount per series of incidences and per annum, and on the other hand, by excluding:

> '...direct or indirect loss of profits, business or anticipated savings and indirect or consequential loss or damage or for any destruction of data' (BT, 2000b).

The serious problem of obtaining insurance coverage might convince the court to uphold such clauses as 'reasonable'. However, the limitation to a specified sum per series of incidences and per annum might be viewed as a **particular complex exclusion or limitation of liability**, since it is nearly impossible for the relaying party to predict whether the limit set by the CA has been reached or exceed through previous incidences which also caused loss. It remains therefore to be seen which approach the courts will follow.

Similar argumentation, as put forward above, may be advanced under the Unfair Terms in Consumer Contracts Regulations 1994 (UTCCR) and its 'test of fairness'.

Special Case - Clauses Which State Maximum Limits of the Value of Transaction or Limit the Purposes of Usage of a Certificate

Let us turn now to the clauses which set out a certain limit for the value of the transaction or clauses which exclude certain kinds of usage. One must ask whether such a statement has the effect that no liability arises at all if the certificate is used in a transaction which, for example, exceeds the permitted transaction limit, or whether the limit stated in the certificate is the limit of liability even if the relying party's loss is in fact greater (Reed, 2000a). In other words, do such clauses limit the contractual duty so that no breach will occur when the relying party ignores these limits and suffers loss or do they merely limit the liability in the event of a breach of the contractual duty? One should distinguish two situations:

If a certificate is limited to a certain transaction value and this limitation has been brought to the attention of the relying party, there is no foreseeable reason why this situation should be treated as limiting the contractual duty to the effect that no liability at all would arise. A reasonably prudent relying party understands a certificate with a transaction limit as a validation of the electronic signature of the holder **up to and including** the limit of the transaction value - not beyond (Reed, 2000a, 145). What sense would it make to hold a CA liable, assuming that the maximum transaction value limit is £ 100, if the actual value of the transaction is £ 99, while denying **any** liability if the actual value amounts to £ 101? The CA knew that it would have to answer for loss caused by the inaccuracy of the information contained in the certificate up to and including the transaction limit. If the holder uses the certificate for transaction worth more than € 100, he knows that everything what goes beyond this sum will not be covered. Thus, this paper suggests interpreting such clauses as limiting the liability only. This interpretation has also the advantage that it might be in line with the *EC Directive on a Community framework for electronic signatures* which states in Art. 6 (4):

> *'Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a **limit on the value of transactions** for which the certificate can be used, provided that the limit is recognisable to third parties. The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded'* (emphasis added).

Although the wording of the directive is, to some degree, ambiguous, the view presented in this paper is supported by the *DTI* consultation paper (DTI, 2001a) as well as the respective implementation of the EC Directive in German law (§ 11 *SigG*).

If a relying party accepts a certified electronic signature even though the party knows that the signature is not good for the use in question, one might ask whether there is any reason to impose liability on the CA. If the relying party entered into dealings with the holder in full knowledge of the 'non-certification' of the use in question, the relying party is not worth protecting. Thus, limitations on use reduce the contractual duty owed. The Electronic Signature Directive in Art. 6 (3) seems to follow the same logical reasoning.

Legislation is necessary in order to comply with Art. 6 (3) and (4) ESD, which apply to qualified certificates only.

Proof and Burden of Proof

The present English rules of contract require the relying party to prove the failure of the CA to take reasonable care. The complexity of technical processes and the ignorance of the organisational structure of a CA will make it more difficult or even impossible for the relying party to prove a breach of a contractual duty and its causality for the loss suffered. These problems have been acknowledged by the EC Directive for the category of qualified certificates. It reverses the burden of proof for qualified certificates. Thus, the British Parliament should therefore take legislative action, at least regarding these certificates, in order to comply with the EC Directive, which states:

> *'As a minimum, Member States shall ensure that ... public a certification-service-provider is liable ... unless the certification-service-provider proves that he has not acted negligently'.*

However, it is unclear whether the rule set out in the Directive is of contractual or tortuous nature, or even of both. This paper is of the opinion that it is sufficient for a proper implementation that the Parliament chooses whether it implements this reversed burden of proof either in contract or tortuous law. The latter might be more appropriate since the language used in the provision seems to hint towards a tortuous rule.

4.1.2 Contractual Relation CA - Certificate Holder, Contract for the Benefit of a Third Party

One of the fundamental norms of English contract law is that, in general, third persons cannot sue for the carrying out of promises made by the parties to a contract (privity of contract) (Treitel, 1999, 540, 559).

However '[a] general and wide-ranging exception' to the common law doctrine has been created by the Contracts (Rights of Third Parties) Act 1999. Under subsection 1 (1) (a) of the 1999 Act, a third party can enforce a term of the contract if 'the contract expressly provides that he may' or under subsection 1 (1) (b) if 'the term [of a contract] purports to confer a benefit on him'. The latter, however, is subject to subsection 1 (2). The third party does not have the right 'if on a proper construction of the contract it appears that the [contracting] parties did not intend the term to be enforceable by the third party'. Express provisions which would entitle the relying (third) party to enforce a term of the contract may be rare. In practice, the opposite situation is more likely as, for example, the form contract for BT TrustWise Class 1 Personal Digital Certificates shows. Third party rights might be expressly exempted. This case is recognised in subsection 3 (2) of the 1999 Act. Thus, the CA can rely on any matter that 'arises from or in connection with the contract [between the contracting parties] and is relevant to the term'. This may well serve the CA as a defence against the third party. Claims based on a purported contract for the benefit of a third party are unlikely to succeed.

4.2 Liability in Tort

4.2.1 Negligent Misstatement

Having examined the contractual liability, attention must now be turned to the liability in tort which may arise, independently of contract. The CA could owe a duty of care to provide accurate information about the identity or other attributes of a holder re-cited in the certificate to a relying party. In the event of a breach of the above mentioned duty the CA would be guilty of negligent misstatement. The negligent misstatement may occur in many ways. The most obvious of which are: the relying party has obtained a copy of the incorrect certificate from the web site of the CA or the holder themselves has sent it together with the electronic document.

This paper will focus in particular on two issues. Firstly, the fundamental question of whether a duty of care is owed by a CA towards a relying party is asked. Since there has been no direct analogy to any previously adumbrated duty of care it is likely that the elaboration of this issue will prove to be crucial. In this connection one must also bear in mind that losses resulting from an inaccurate certificate are almost always going to be purely economic. Recovery of economic loss is fraught with difficulties (Nicoll, 2000, 25) and bears the inherent fear of:

> '... liability in an indeterminate amount, for an indeterminate time, to an indeterminate class'.

Secondly, this paper will explore the standard of care to be expected.

Duty of Care

> 'The modern approach to deciding whether a duty of care exists - some speak also about an 'assumption of responsibility' when pure economic loss is involved - invokes applying one or more of three tests based on: (a) foresight; (b) proximity; (c) considerations of justice and reasonableness in imposing the duty'.

The two latter tests might play the most crucial role in establishing a duty of care, which rests ultimately on social and civic responsibility.

The Test of Proximity

The loss caused by reliance on an incorrect certificate will almost in any case be economic. The test of proximity has been proved to be an important part in the reasoning in many of the cases concerning the extent of liability for economic loss causes by negligent misstatement (Harpwood, 2000, 32). This view was expressed in particular in *Hedley Byrne & Co. Ltd. V. Heller & Partners Ltd.* A duty of care would exist in relation to statements only if there is a 'special relationship' between the parties, a relationship of close proximity (Rogers, 1994, 292), which amounts to an 'equivalent to contract'. The circumstances where such a relationship has been found are rare although not unknown. Lord Oliver in *Caparo Industries plc v. Dickman* described the necessary relationship as typically having four characteristics:

> *'the advice is required for the purpose, whether particularly specified or generally described, which is made known, either actually or inferentially, to the adviser at the time when the advice is given;*
>
> *the advisor knows, either actually or inferentially, that his advice will be communicated to the advisee, either specifically or as a member of an ascertained class, in order that it should be used by the advisee for that purpose* [];
>
> *it is known, either actually or inferentially, that the advice so communicated is likely to be acted upon by the advisee for that purpose without independent inquiry; and*
>
> *it is so acted upon by the advisee to his detriment'.*

The CA knows that the information contained in the certificate is required and relied upon to link a public key to a person, whose identity or other attributes are certified (ABA, 1996, Comment 2.2.1). It is fully aware of the fact and necessity that the certificate will be communicated to any relying party. The advisee will base his decision to transact with the holder upon the validity of the certificate and the information it contains. It seems that the conditions set out in the '*Caparo* test' are met.

Concerning the range of persons to whom a duty is owed, it was held that it is not necessary that the defendant knows the identity of the potential plaintiff. But what is the position where information is foreseeably relied on by a larger group of persons? In our case, the statement (certificate) issued by the CA is put into more or less general circulation. One must bear in mind in particular that the economic loss which might be caused can be enormous. That the size of the class to which the recipient of the statement belongs is a crucial criterion for the acceptance or denial of a duty of care was expressed in *James McNaughton Papers Group Ltd. v. Hicks Anderson & Co.* by Lord Justice Neil. Lord Bridge, trying to define the outer boundaries of the concept of duty of care, argued in *Caparo Industries plc v. Dickman* that to hold the adviser liable in these situations in which strangers rely foreseeably on the statement (here certificate) for any of a variety of different purposes, which the maker of the statement had no specific reason to anticipate, would mean to subject the maker of the statement (here the CA) to 'liability in an indeterminate amount, to an indeterminate class'. However, the purpose of issuing the statement (certificate) is to provide a link between a public key and a person, whose identity or other attributes are certified. The recipient of such a statement relies upon this certified unique link and a CA has every reason to anticipate the purpose of its certificate. Thus, the CA would owe a duty of care if the courts were prepared to follow this argumentation. Furthermore, one may argue that the relationship between the CA and the relying party falls just short of contractual privity or even amounts to a contractual relationship, as shown above in section A. I. Therefore, a 'special relationship' between the CA and a relying party might exist.

The Test of Fairness, Justice and Reasonableness - Policy Arguments

Considerations of what is fair, just and reasonable are in reality very often co-extensive with policy arguments (Harpwood, 2000, 33). Policy reasoning may, however, also be seem as an independent test. The following factors could influence the judicial decision. In favour of ascertaining a duty of care it may be invoked that the CA is in a better position to insure any loss and can therefore best afford to bear the loss. Also the notion of protection of consumer interests by means of a strong liability regime might support the adoption of a duty of care. However, as shown above, the insurance coverage is apparently not unlimited and the potential amount of damages, which might be claimed, could be enormous, due to wide circulation of a certificate. There is still the threat that the courts would interpret the class of potential 'advisees' as too indeterminate and, thus, deny a duty of care. Also the practical consideration to facilitate the growth of electronic communication and commerce by restricting liability of e-businesses might play a certain role. Once again, it remains to be seen which arguments the courts will follow.

Breach of the Duty of Care - Standard of Care

Even if the courts are prepared to accept a duty of care, uncertainty remains as to the standard of care. 'Reasonable care' is the standard against which liability for negligent misstatement is most often measured. Viewed from a business perspective, reasonable care means that degree of care that an ordinarily prudent and competent person engaged in the same line of business or endeavour would exercise under similar circumstances. However, in an industry as novel as that of CAs appropriate standards of reasonable care have not been established yet. Therefore, the standard of care owed to the relying party will be defined to great extent by the representations the CAs make about the level of inquiry they promise to carry out before issuing a certificate. The certificate, the certification practice statement (CPS) and in a sense, therefore, the contract between the CA and the holder of the certificate define the tort. The more care the CA promises to apply, the more qualified and skilled personnel it will probably use and thus the standard of care will increase. The technology and software used will also have an influence on the standard of care. As a consequence, it appears that the CA will need to consider the anticipated use of the certificate it issues, and ensure that its procedures, technology and personnel are appropriate in the light of those uses (Schmedinghoff, 1998, 4.2.1). Policy considerations, like in the concept of duty of care as advanced above, will certainly be involved.

Quantum - Value of the Claim - Damages

The basic principle is that the claimant must be restored to the position he would have been in if the tort had never been committed (Harpwood, 2000, 451). However, the CA will only be liable for damages which a reasonable person could have foreseen (test of remoteness of damages). In cases involving economic loss, the authority is *Liesbosch Dredger v. SS Edison*. The foreseeability of loss is narrowly construed in such cases. Additionally, policy considerations may play a role. It is likely that the foreseeability of damages is interpreted even more narrowly in order to limit the liability of CAs to an extent which may possibly be covered by insurance contracts. *Reed* even suggests that direct 'loss of transaction value only' will be recoverable.

However, it is unlikely that CAs will leave the extent of damages possibly awarded to the general rules. CAs try to disclaim responsibility by excluding and/or limiting liability in the event of breach of a duty of care. In some cases, however, the Unfair Contract Terms Act 1977 may bar this escape route. The disclaimer becomes subject to the test of reasonableness. In general the same arguments as advanced above apply here.

Proof and Burden of Proof

The general rule is that a plaintiff has to prove on a balance of probabilities that the defendant has been negligent. This might be a cumbersome or even an impossible task due to the complexity of technical processes and the ignorance of the organisational structure of a CA. Finally, the *EC Directive on a Community framework for electronic signatures* (Art. 6 (1), (2)) requires for qualified certificates that the CA has to prove that it did not act negligently. Therefore, the present English rules need to be brought in line with the EC provisions (see also DTI, 2001a), as already outlined above.

4.2.2 Deceit

On the very rare occasion, therefore mentioned here only sketchily, that the CA should provide incorrect information, e. g. contained in their certificates or in its certificate revocation list, with fraudulent intention, the injured third party might sue the CA in an action for deceit. The requirements are that the defendant knowingly or recklessly made a false representation to the plaintiff intending him to act on the representation, and that the plaintiff did act on it to his detriment (Jones, 2000, 94-5). In particular, the defendant must have intended the plaintiff, or a class of persons, to which the plaintiff belongs, to act on the representation, but where a representation is found to have been made fraudulently there is a rebuttable presumption that the representor intended the plaintiff to rely on it.

4.2.3 Vicarious Liability

For the sake of completeness vicarious liability must also be mentioned. In the previous chapters this paper stated that 'a CA' commits a tort. This is, however, not precise. The tort is usually committed by an employee of the CA. In many cases this employee will not be able to cover the loss caused by his wrong. His employer, here the CA, can in general better afford to bear the cost of compensating the injured third parties. Thus, the courts developed the tort of vicarious liability (Harpwood, 2000, 345). The essential requirements of this tort are (a) a tort; (b) committed by an employee; (c) who was acting in the course of his employment (Jones, 2000, 381).

4.3 Summary So Far

Several hurdles must be overcome before one is able to construe and rely on a **contract between the CA and the relying third party** which would, in some way, warrant the accuracy of the certificate.

Firstly, two possibilities of constructing such a contract have been suggested. One of the two suggested constructions requires **direct communication** between the two parties, although this might not always be the case. The other construction carries the risk that the relying party might be unaware of the unilateral offer of the CA. It remains to be seen whether or not it is sufficient that the offeree (relying party) does not actually know that the offeror (CA) does not have any such intention. Furthermore, the **requirement of consideration** for the promise to provide accurate information is only then satisfied if one is prepared to accept the general enhancement of the certificate market as a form of consideration.

Secondly, concerning the terms of contract, it has been suggested that only reasonable care is owed, but what 'reasonable care' means in the particular case depends largely on the representations made by the CA. The scope of the contractual duty, therefore, may largely be defined by the CA.

Thirdly, the **enormous financial risk** might encourage the courts to adopt a narrow approach towards foreseeable damages, and a generous approach towards the restrictive control of exemption and limitation clauses. Ultimately, it will be a question of policy. The courts have to find a balance between strengthening the confidence of customers (i.e; consumers) in e-commerce through a strong liability regime, and to facilitate a robust growth of e-commerce businesses by keeping liability risks low.

Fourthly, the relying third party has the **burden of proof**. The complexity of technical processes and the ignorance of the organisational structure of a CA will make it more difficult, and in some cases even impossible, for the relying party to prove a breach of a contractual duty and its causality for the loss suffered.

A claim based on a **contract for the benefit of a third party** is very unlikely to occur. Regularly such intent is expressly exempted in the certification contract between the CA and the certificate holder.

The following obstacles may hinder a **tortuous claim based on negligent misstatement**:

Firstly, it might not be easy to establish a **duty of care**. On the one hand, the range of persons to whom a duty is owed is difficult to anticipate and, thus, the threat of **liability in an indeterminate amount, to an indeterminate class** emerges. On the other hand, the relation between the CA and the relying party falls short of contractual privity. The question of who is in a better position to bear the loss, as well as policy arguments, may also play a role in adopting or denying a duty of care.

Secondly, the potential plaintiff enjoys a wide freedom to disclaim liability, subject 'only' to the 'test of reasonableness' of the Unfair Contract Terms Act 1977.

Finally, the plaintiff has the **burden of proof** which aggravates his position, as already outlined above.

A **tort based on deceit** has almost **no practical significance** and, moreover, the **burden of proof** on the site of the plaintiff may render a claim short of impossible. Based on the fault of the servant, vicarious liability under English law on its own appears to be unproblematic.

5. The Present Liability Regime in Germany

5.1 Contractual Liability

5.1.1 Contractual Relationship CA - Relying Third Party - Contract of the Provision of Information **('Auskunftserteilungsvertrag')**

The German Civil Code *('Bürgerliches Gesetzbuch (BGB)')* sets out in § 676 *BGB* (recently re-numbered § 675 (2) *BGB*) the presumption that the giving of advice, in our case provided in the form of a certificate containing information about a link between a public key and certain attributes of a subject, is regarded as a non-committal social favour, which is not intended to create legal relations. However, this presumption may be 'rebutted'. The recovery of loss, caused by reliance on an inaccurate certificate, is possible if the courts find themselves able to construe a contract, expressed or implied, between the CA and a potential relying party, which would oblige the CA to give accurate information about the link between a public key and the identity or other attributes of a subject in their certificates (contract of the provision of information (*'Auskunftserteilungsvertrag'*). If the information proved to be incorrect, the CA would be liable for breach of contract.

Offer* (*'Angebot*') *and acceptance* (*'Annahme'*) *- Missing 'Rechtsbindungswille'?

As English law, the German law also requires offer (*'Angebot'*) and acceptance (*'Annahme'*) in order to form a valid contract. Both offer and acceptance are so-called declarations of intention (*'Willenserklärungen'*). A *'Willenserklärung'* consists out of two components:

(1) the external declaration (*'Erklärungstatbestand'*) and

(2) the internal intention (*'Wille'*).

If one of the two components is missing, there is no *'Willenserklärung'*. To establish the *'Erklärungstatbestand'*, by means of interpretation (*'Auslegung'*), the courts will ask whether a reasonable prudent recipient understands the declaration of intention (*'Willenserklärung'*) voiced by the declarer as intending to create a legal consequence (*'Rechtsfolge'*);more precisely, whether a reasonable prudent recipient can infer from the declaration.

(1) the will of the declarer to act at all (*'Handlungswille'*),

(2) the will to create a legally binding relationship in general (*'Rechtsbindungswille'*) and

(2) the will to engage in the particular transaction (*'Geschäftswille'*).

As stated above, the general presumption set out in § 676 *BGB* (re-numbered § 675 (2)

BGB) is that a party who gives advice lacks the intention to create a legally binding relationship, thus, lacks *'Rechtsbindungswille'*. However, if the declarer, in our case the CA, does expressly state that it wants to be held liable towards third parties for the accuracy of the information contained in the certificate then there will be apparently a *'Rechtsbindungswille'*. To find such a statement in practice might be rather unlikely. It is not necessary, however, that the *'Rechtsbindungswille'* (and all other necessary 'wills') are expressly stated. The *'Rechtsbindungswille'*, and ultimately the contract, can be derived from conduct implying an intent to effect a change in legal position (*'schlüssiges Verhalten'*). Whether the court is able to imply *'Rechtsbindungswille'* depends decisively on the circumstances of the particular case. It is sufficient that the adviser is able to foresee (objective criterion), according to the Federal Supreme Court (*'Bundesgerichtshof (BGH)'*), that the advice given is of considerable importance for the advisee; and the advice must serve as the basis for fundamental decisions. Expert knowledge in providing the information in question, and the advisor's own economic interests in providing them, might be seen as one strong indicator for a *'Rechtsbindungswille'.* Another indication of such a will is that the information has been provided for consideration. It is, however, not necessary that the consideration has been provided in the form of remuneration (*'Entgelt').* The gain of some sort of economic benefit is sufficient. As already stated in the previous sections, a CA knows that the information contained in the certificate is required and relied upon so as to link a public key to a person, whose identity or other attributes are certified (ABA, 1996, Comment 2.2.1, p.61). It is fully aware of the fact and necessity that the certificate will be communicated to any relying party. The advisee will base his decision to transact with the holder upon the validity of the certificate and the information it contains. A CA can be seen as having accumulated considerable expert knowledge in providing certificates, since it is the essence of its business and it will apparently gain economic benefits from providing certificates which are shown to third parties.

Furthermore, it is not even necessary that the advisee (relying party) has direct contact with the adviser (CA). Therefore, the relying party may also receive the certificate from its holder. However, the adviser must anticipate the group of potential advisees. No contract will be implied if the group of potential advisees is not sufficiently defined. In particular, if an advice was given without remuneration (*'Entgelt'*), it cannot be expected that the adviser accepts liability for enormous economic risks (Larenz and Wolf 1997, § 22, margin number 39). As outlined in the sections concerning English Law, the risks, for the CA to expose itself to an enormous liability risk, is imminent. Thus, the German courts will probably decline to construe an '*Auskunftserteilungsvertrag'.*

5.1.2 Contractual Relationship CA - Certificate Holder - Contract with a Protective Effect Towards a Third Party ('Vertrag mit Schutzwirkung zugunsten Dritter') (See Figure 6)

Another possibility to subject a CA to contractual liability is to interpret the certification contract between the CA and the certificate holder as having a protective effect (*'Schutzwirkung'*) towards a party who relies on a certificate. The jurisdiction developed this remedy in order to protect a third party, which suffers loss because a contract, to which he is not party, but to which he enjoys a relationship of close proximity, has not been performed properly. The third party is regarded as worth protecting, since in many cases the available remedies based on tortuous liability remains behind those based on contractual liability. Each contract contains so-called primary or main obligations, e.g; in a sales contract to deliver the goods, and secondary obligations, first and foremost the obligation to exercise due diligence or due care (*'Verplichtung zu sorgsamen Verhalten'*) while performing the contract.

Due to the close proximity, the third party becomes, beside the creditor, an 'additional' creditor of the secondary contractual obligation (*'sekundärer Leistungsanspruch'*) to exercise due diligence or due care while performing the contract. If the debtor fails to exercise due care, in particular when he fails to perform his primary obligations, the third party can sue the debtor for breach of contract, more precisely for breach of a secondary performance obligation.

To construe a contract in the way as having a protective effect towards a third party, high standards must be met since being subject to contractual liability increases the liability risk enormously. If the parties have not expressly agreed on a protective effect of the certification contract, the following criteria, set out by the courts, must be met:

Firstly, the third party must come in contact with the obligation to be performed *('Leistung')* in the same way as the creditor. This must have been intended by the contracting parties. A mere coincidental contact is not sufficient. In practice a CA accepts to perform several duties with which third parties are intended to come in contact. The most obvious are: the issuance of the certificate which properly identifies a subject or establishes other attributes of him and links these facts to a public key; and the maintenance of a web-based list of all issued certificates as well as the publication of a certificate revocation list. Each of these obligations to be performed is intended to be used by the third party, even if the CA performs because it is obliged to do so towards the certificate holder.

Secondly, the creditor (certificate holder) must have a legitimate interest *('berechtigtes Interesse')* in the performance of the contract in due care also in relation towards a third party. A legitimate interest is given, according to the *BGH*, if the certification contract can be interpreted as recognising the intention to benefit a third party *('Drittbegünstigung').* The certificate holder has an interest in a protective effect of the certification contract to the benefit of the relying party since the reliability of the certificate and all 'connected' services, i. e. the certificate revocation list, are of decisive importance for the relying party. Thus, the proper performance of the certification contract shall directly benefit the third party.

Thirdly, it is necessary that the group of people to whom the contractual duty to take due care is owed is - from an objective point of view - identifiable by the debtor. In other words the liability risk must be assessable, calculable and if need be insurable in order to impose the contractual liability regime - without any additional consideration - upon the debtor (Jagmann, 1995).

This point is controversially discussed in a small academic circle; however a judgement concerning CAs has not yet been handed down. *Ms. Leier* argues that since the CA knows that the purpose of concluding the certification contract is to obtain a certificate which is communicated to innumerable third parties in order to provide proof of identity or of other attributes; it can prepare itself for being liable to a potentially large group. The more obvious the interest of the creditor in the protection of a third party is, the less necessary it is to demand an identifiable class of third parties. This interpretation, however, is not convincing. It neither finds a foundation in the existing case law nor does it seem to understand the potential of the new technology to create enormous loss. It is true that the *BGH* does not require that the debtor must anticipate the names or the number of third parties. This has been held in cases involving halls, gymnasiums and stadiums. However in all of these cases some limitation was provided by the maximum capacity of these buildings. In contrast, an unreliable certificate can cause loss to - in theory - millions of people in no time. There are no walls in cyberspace. Ultimately, the courts will focus on the special circumstances in each case and will then decide whether a certain group was, or was not, identifiable by the debtor. This is the question of whether it is reasonable (or just and fair) to subject the debtor to contractual liability and, thus, to increase his liability risk. The author of this paper answers this question in the negative, out of the above given reasoning. In conclusion so far, a claim based on a contract with a protective effect towards a third party is unlikely to succeed under existing law.

5.2 Liability in Tort ('Deliktische Haftung')

The German *BGB* generally, tries to restrict claims in tort from the very outset. Pure economic loss *('reiner Vermögensschaden')* is not protected generally, but only in special circumstances. Since the loss caused by an incorrect certificate will be in most cases economic loss, this section will only focus on those paragraphs of the *BGB* which allow the recovery of *'Vermögensschaden'*.

5.2.1 Liability in Tort Based on Intention ('Deliktische Haftung bei Vorsatz')

§ 823 (2) BGB in Connection with § 263 German Criminal Code ('Strafgesetzbuch (StGB)')

Liability under § 823 (2) *BGB* arises when a law 'designed to protect another' is culpably contravened. Protective statutes in this sense include all rules of private and public law, especially criminal law (Zweigert and Kötz, 1998, 602).

For our purposes § 263 *StGB* (fraud = *'Betrug'*) might be most relevant. Thus, if an employee of a CA commits a fraud towards the relying party, the former will be held liable for the consequential economic loss. The relying party has to prove the facts, culpability, the loss caused and causality (Thomas, nd, § 823, margin number 167), which is predominantly a difficult undertaking (Leier, 2000, 16). If (and a big if) successful, the plaintiff is entitled to be put into the position in which he would have been if the fraudulent statement had not been made. In practice, however, fraudulent behaviour is unlikely to occur.

§ 826 BGB

§ 826 *BGB*, protecting all legal interests, i.e. economic loss, provides that a person is liable if he intentionally causes harm to another in a manner that is *contra bonos mores*.

Boni mores is a flexible and changing notion, which refers to a minimum set of legal-ethical principals (*'rechtsethisches Minimum'*) seen as a set of legal value assessments (*'rechtliche Wertungen'*) (Larenz and Canaris, 1994, § 78 II 1). The courts have used this provision to impose liability in a diverse range of cases where one party has caused harm to another by behaviour so offensive and improper as to incur strong disapprobation from the average person in the relevant section of society (Zweigert and Kötz, 1998, 603). This provision, therefore, covers multitudes of wrongs under one broad and abstract formula and is better described as 'field of tortuous liability' than as tort (Markesinis, 1994, 895-6). One line of case law has been developed as to impose liability upon a person who intentionally gives false information (deceit = *'Täuschung'*), aware of the **consequences** of his conduct, which he accepts as inevitable even though he may not specifically desire them ('*Schädigungsvorsatz'* in the form of *'dolus eventualis'*). If the plaintiff is not able to prove 'deceit', the aspect of recklessness *('Leichtfertigkeit')* in providing of information (e. g. about the creditworthiness of another party) might play a decisive role in cases involving special professional skills. A CA's personnel, certainly has the sort of professional skills, already been outlined above. Consequently, if an employee of a CA recklessly misstates the identity, or other attributes of a subject, in a certificate and is aware of the consequences of his conduct, namely that a relying party will base his decision whether or not to transact on these information and, therefore, could suffer harm, then the CA may be liable under § 826 *BGB*. However, even if the plaintiff is able to establish a reckless misstatement (*'fahrlässige Fehlinformation'*), in most cases to prove *'Schädigungsvorsatz'* might be a hurdle too high to overcome.

5.2.2 Liability in Tort Based on Negligence **('Deliktische Haftung bei Fahrlässigkeit') - *§ 831* BGB *in Connection with Either § 823 (2)* BGB, *§ 263* StGB *or § 826* BGB**

Usually an employee will not be able to cover the loss caused by his 'unlawful act'. It is therefore desirable to seek redress from his employer, who is generally in a better position to make provisions for such incidences. § 831 of the German Civil Code regulates what Common lawyers call 'vicarious liability'. It states the following:

> *'(1) A Person who employs another for work is obliged to make compensation for the harm which the other inflicts unlawfully on a third party in the carrying out of the work. The duty does not arise if the employer observes the care necessary in the affairs of life in the choice of the person employed and, insofar as he has to provide apparatus or implements or to supervise the carrying out of the work, in such provision or management; or if the harm would still have arisen despite application of this care.*
>
> *(2) ...'*

The German Civil Code based a master's liability on **his** fault of bad selection, instruction and/or supervision of his servants, as well as the proper provision with the right kind of equipment. It is worth stressing that § 831 *BGB* makes no mention of *culpa* (fault) in relation to the 'unlawful' act committed by the employee! The 'unlawful act' here may be seen as a fraudulent act (§ 831 *BGB* in connection with § 823 (2) *BGB*, § 263 *StGB*) or as an act *contra bonos mores* (§ 831 *BGB* in connection with § 826 *BGB*), as outlined above.

The master will be presumed at fault and will be made liable unless he shows that:

> (a) he was careful in the selection, instruction and training of his servants and that he properly supplied them with the right kind of equipment or, failing that,
>
> (b) the damage or injury would have occurred even if the master had fulfilled the above mentioned duties, § 831 (1) 2nd sentence *BGB*. Where large organisations are concerned, the jurisdiction has developed the so-called 'decentralised exoneration' (*'dezentraler Entlastungsbeweis'*).

It allows the master to show that the selection of the 'leading employees', who stand in the hierarchically intermediate position had been properly chosen and supervised. In practice, in most of the cases the possibility of exoneration will lead to exclusion of liability (Leier, 2000, 16).

5.3 Summary So Far

A claim based on the construction of an ***'Auskunftserteilungsvertrag'*** will most likely fail because of the missing *'Rechtsbindungswille'*. Even if under German law direct communication between the contracting parties is not required, the group of potential advisees is not sufficiently defined to expose the CA to contractual liability. If advice was given without remuneration, the adviser it cannot be expected to accept liability for **enormous economic risks**.

The second possibility in German law to subject a CA to contractual liability is to interpret the certification contract between the CA and the certificate holder as having a protective effect towards a party who relies on a certificate (*'Vertrag mit Schutzwirkung zugunsten Dritter'*). A claim based on the above mentioned contract, however, does not appear more likely to succeed. The notion that **liability must be assessable, calculable and eventually insurable** plays an important role. Although controversial, the author of this paper is of the opinion that the group of people, who are intended to be included in the protective effect of the contract, is too indeterminate as to facilitate the CA to assess, calculate, or insure the liability risk.

Tortuous liability for fraud (§ 823 II *BGB* in connection with § 263 *StGB*) as well as **liability for conduct *contra bonos mores*** (§ 826 *BGB*) is based on intention and is, therefore, **unlikely to arise in practice** since most incorrect statements in certificates are caused negligently. However, even if the fraudulent conduct or conduct *contra bonos mores* was committed intentionally, the **burden of proof** might be an effective bar to succeed with a claim.

Vicarious liability, which in German law is based on the fault of the master, arises only if the master fails to exonerate himself, which is, in practice, an unlikely event.

6. Misplaced Confidence? - Comparison of the Legal Systems and Final Evaluation

This chapter will attempt to discover the common grounds and differences between the English and German law. What the paper, due to its scope, however, cannot provide is a sophisticated abstract comparative analysis of the general issue of professional liability for provision of information towards third parties. Comparison is only used here as a method to offer a initial explanation of whether, and why, it might be more likely to succeed with a claim against a CA in the courts of one or the other jurisdiction.

We will eventually turn our attention to whether the legal protection of relying third parties is sufficient to be able to speak about a source of trust, and if the legal protection lacks this quality, what alternative suggestions may be considered.

6.1 Remedies Requiring Wilfulness (Intention)

If the plaintiff bases his claim on tortuous remedies requiring intention, the legal position in which he will find himself placed, is similar in England and Germany. Despite the fact that intentional misstatements in certificates or certificate revocation lists are rare, the burden of proof is in both jurisdictions imposed upon the plaintiff. As stated above, this hurdle will certainly be the strongest hindrance to a successful claim, recalling the complexity of technical processes and the ignorance of the organisational structure of a CA.

6.2 Negligent Misstatement and its German Counterpart

In German and English law liability for negligent provision for incorrect information. and options causing pure economic loss is dealt with by different means. Apart from § 826 *BGB,* the German law deals with the above predominantly by means of the law of contract (i. e. the contract with protective effects towards third parties *('Vertrag mit Schutzwirkung zugunsten Dritter'))*; while English law treats this as a tort problem (negligent misstatement). The different means of solving negligent misstatement problems is easily explained. In German law the concept of the *'Vertrag mit Schutzwirkung zugunsten Dritter'* was developed, because the law of torts, at least in principle, provides no remedy if pure economic loss is caused negligently (Lorenz, 1994, 70). The contract with protective effect towards third parties

> '...is essentially noting other than a tortuous safety valve: the greater the pressure, the more legal confidence is transferred to contract law' (von Bar, 1994, 100).

In English law this issue has been treated as a tortuous one, since the doctrines of consideration and privity of contract have regularly rendered claims in contract impossible (von Bar, 1994, 100). However, the problems the judges are facing and the adopted solutions are quite similar (von Bar, 1994, 100). The crucial question, especially in the case of a CA, of how far one should expand the sphere of protection towards third parties demands an answer in both legal systems. In order to establish a duty of care, the

English law asks for a **relationship of close proximity** between the adviser and advisee - the '*Caparo*-test'. It tries to limit the potential group of protected parties by stating that the information can be relied on only for the purpose within which it was supplied, in order to **prevent liability in an indeterminate amount to an indeterminate group**. The German law questions whether the **group of persons to be contractually protected is capable of description by objective standards**. If the group of persons becomes too large, however, the notion that the **liability is not assessable, calculable, and eventually insurable** will lead to an exclusion of contractual liability.

Obviously, the two approaches are closely related (i. e. the notion that an advisor cannot be held liable towards third parties if the liability risk becomes an 'existential threat' to him). Returning, however, to the concrete situation of third parties relying on inaccurate certificates, a decision in Germany and England might differ. In England, the law looks at the relationship between the advisor (CA) and the (relying) third party; whilst German law asks whether there is a sufficient link between the creditor of a contract (certificate holder) and the (relying) third party (von Bar, 1994, 123). The differing focal point might enable an English court of law to lay a stress on the additional fact that the relationship between the CA and the relying party is, or is almost, of contractual nature. This additional fact could convince English courts to impose a duty of care upon a CA.

6.3 Dead End 'Contract' - The Construction of a (Genuine) Contractual Relation Between the Advisor and a Third Party

To establish a 'direct' contractual relation between a CA and a relying party constitutes problems in both jurisdictions. English and German law have developed indicia through which to distinguish contracts from any other agreement of a non-binding character. The English legal system created the 'concept of consideration', while the German system deals with this issue by the means of *'Rechtsbindungswille'* (Zweigert and Kötz, 1998, 399). It is worth mentioning again that the contract with protective effect towards third parties does not fall under this headline since, strictly speaking, a contract with protective effect towards third party constitutes contractual liability without a contract (von Bar, 1998).

> 'An Englishman is liable, not because he has made a promise, but because he has made a bargain' (Furmston, 1996, 28).

This bargain, as shown above, may result from the general enhancement of the market for a certain product or service. Conversely, German law seems to deny an intention to create a legal relationship if the liability risk and the consideration are gravely disparate. The remote chance of the enhancement of the market will not suffice; remuneration is necessary to subject someone who gives some sort of advice to a contractual duty.

Irrespective of any exemption clauses, therefore, liability of a CA for inaccurate statements in its certificates, caused negligently, is (slightly) more likely to occur in England than in Germany.

6.4 Burden of Proof

Overall, one might not forget that:

> '... most claims [in both jurisdictions] would very likely fail (or would be settled at a very early state in the proceedings) on the grounds that no negligence [or breach of a contractual duty] can be proved or that the causation link between negligent misstatement and the loss has not been established' (Markesinis, 1994, 292).

6.5 Final Conclusions - Liability as Source of Trust and the Need for Regulation

In conclusion, there are many (perhaps too many) minor and major obstacles in both German and English law which question the success of any claim by a relying party. A strong liability regime (which would particularly enhance confidence in **non-qualified** certificates and generally in electronic communication and commerce) is practically not in existence! If the present laws are applied, the question of whether to boost e-commerce through consumer confidence or through low legal obstacles for businesses operating in the respective market seems to be decided in clear favour of the latter one. It is doubtful whether this decision was intended, since relying parties could be deprived of any legal protection.

This paper is, therefore, convinced of the need to find a balance between both conflicting interests, since somebody who takes up trust, as a CA does, must prove reliability (also) through liability (Haas, 1998, 285). If 'the worst' should happen, it is decisive for relying parties to have at least some legal remedy at hand. On the other hand, however, businesses must be enabled to protect themselves against the risk of liability in an indeterminate amount to an indeterminate group.

Since the existing laws in both countries contain many uncertainties and obstacles, (making a success of a relying party's claim unlikely) this paper suggests the introduction of a special tortuous liability rule, which eliminate the two main obstacles for a successful claim:

> the burden of proof imposed upon the relying party; and
>
> the threat of liability in an indeterminate amount, to an indeterminate class, which is owed to the open character of the Internet.

To deal with the first obstacle it may be sufficient to reverse the burden of proof. The CA is in a (much) better position to prove that it has not acted negligently, since it is familiar with technology and its own organisational structure. In order to tackle the second obstacle, two equally important measures may be suggested. On the one hand, there might be introduced a new statutory tort, subjecting the CA to liability for non-qualified certificates similar to the EC Directive. The courts would no longer be troubled by the notion of liability in an indeterminate amount, to an indeterminate class while establishing a duty of care (England), or a protective effect of the certification contract towards relying parties (Germany), since liability is imposed by statute. This, however, would solve the legal, but not the factual problem of liability in an indeterminate amount, to an indeterminate class. Therefore, to enable businesses to manage effectively the enormous liability risk one may expressly permit by statute exemption and limitation clauses which intend to limit the liability to a certain amount per annum and/or per series of incidences, coupled with a minimum amount of liability, which would cover ordinary incidences and would prevent abuse of these exemption clauses.

A call for harmonisation (on an European level) might be premature, since one must first consider the other jurisdictions within Europe.

Bibliography*

American Bar Association (ABA) (1996), *Digital Signature Guidelines - Legal Infrastructures for Certification Authorities and Secure Electronic Commerce*, American Bar Association, Chicago.

Angel, J (1999),*Why use Digital Signatures for Electronic Commerce?,* Journal of Information Law and Technology, 1999, (2) <http://www.law.warwick.ac.uk/jilt/99-2/angel.html>.

Atiyah, P S (1995), *An Introduction to the Law of Contract*, 5th ed; Clarendon Press, Oxford.

Bassenge, P, Diederichsen, U, Edenhofer, W, Heinrichs, H, Heldrich, A, Putzo, H, Sprau, H, Thomas, H (1999), *Palandt - Kurzkommentar zum Bürgerlichen Gesetzbuch*, 58th ed., Verlag C H Beck, München, Munich.

Beale, H G, Bishop, W D and Furmston, M P (1995), *Contract - Cases and Materials*, 3rd ed; Butterworths, London, Dublin and Edinburgh.

Brazier, M and Murphy, J (1999), *Streets on Tort*, 10th ed; Butterworths, London, Edinburgh and Dublin.

BT (1999), *BT Certification Practice Statement*, BT, <http://www.trustwise.com/repository/PDF/cps.pdf>.

BT (2000), *Conditions for BT TrustWise Class 1 Personal Digital Certificates*, BT, <http://www.trustwise.com/repository/pdf/class1_personal_contract.pdf>.

BT (2000), *BT TrustWise Relying Third Party Charter*, BT, <http://www.trustwise.com/rpa/index.html>.

Cane, Peter (1996), *Tort Law and Economic Interests*, 2nd ed; Clarendon Press, Oxford.

Furmston, M P (1996), *Cheshire, Fifoot and Furmston's Law of Contract*, Butterworths, London,

Department of Trade and Industry (DTI) (1999), *Building Confidence in Electronic Commerce - A Consultation Document*, DTI, <http://www.dti.gov.uk/cii/ecommerce/ukecommercestrategy/archiveconsultationsdocs/index.shtml>.

Department of Trade and Industry (DTI) (2001), *Consultation on EC Directive 1999/93/EC of the European Parliament and Council on a Community Framework for Electronic Signatures*, DTI, London.

DTI (2001), *Consultation on EC Directive 1999/93/EC of the European Parliament and Council on a Community Framework for Electronic Signatures - Summary of Responses*, <http://www.dti.gov.uk/cii/datasecurity/electronicsignature/signatures2.shtml>.

Department of Trade and Industry (DTI) (1999), *Promoting Electronic Commerce - Consultation on Draft Legislation and the Government's Response to the Trade and Industry Committee's Report*, DTI, London.

Dawe, T (2001), *The E-key to Safe Business on the Net*, The Times, 12. June 2001, <http://www.thetimes.co.uk/article/0,,349-2001194780,00.html>.

Der Spiegel Online, (2000), *Bald ohne Kreditkarte Online Shoppen*, Der Spiegel Online, 22/2000, <http://www.spiegel.de/netzwelt/technologie/0,1518,78630,00.html>.

Der Spiegel Online (2000), *Verwaltung Signiert Digital*, Der Spiegel Online, 04/2000, <http://www.spiegel.de/netzwelt/politik/0,1518,61041,00.html>.

Edwards, L and Waelde, C (2000), *Law and the Internet*, Hart Publishing, Oxford and Portland (Oregon).

Fisher, H D (1999), *The German Legal System & Legal Language*, 2nd ed; Cavendish Publishing, London and Sydney.

Froomkin, M A (1996), *The Essential Role of Trusted Third Parties in Electronic Commerce*, Oregon Law Review, 1996 (75) 49.

Gründel, N (2000), *Fineid zum Ersten, Fasme zum Zweiten*, Der Spiegel Online, 23/2000, <http://www.spiegel.de/netzwelt/politik/0,1518,79665,00.html>.

Guest, A G. *et al*. (eds.) (1989), *Chitty on Contracts - General Principles*, 26th ed; Sweet & Maxwell, London.

Haas, L (1998), *Zur Haftung der Zertifizierungsstellen nach dem SigG gegenüber Dritten* published in Heldrich, A.; Schlechtinger, and Schmidt, (eds.) (1998)*, Recht im Spannungsfeld von Theorie und Praxis - Festschrift für Helmut Heinrichts zum 70. Geburtstag*, Verlag C. H. Beck, München (Munich), 261.

Harpwood, V (1996), *Law of Torts*, 2nd ed; Cavendish Publishing, London and Sydney.

Harpwood, V (2000), *Principles of Tort Law*, 4th ed; Cavendish Publishing, London and Sydney.

Harrison, R (2000), *Public Key Infrastructure: Risks of Being Trusted*, 2000 11 C & L 28.

House of Commons - Select Committee on Trade and Industry (1999), *Seventh Report*, Trade and Industry Committee Publications, London.

Howells, G G. and Weatherill, S (1995), *Consumer Protection Law*, Dartmouth Publishing, Aldershot, Brookfield (USA), Singapore, Sydney.

Jagmann, R (1995), *J. von Staudinger - Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen*, vol. containing §§ 328 - 361, 13th ed., Sellier - de Gruyter, Berlin.

Jones, M A (2000), *Textbook on Tort*, 7th ed; Blackstone Press Limited, London.

Larenz, K (1986), *Lehrbuch des Schuldrechts*, 2nd vol., 1st half-binding, 13th ed., Verlag C. H. Beck, München (Munich).

Larenz, K (1987), *Lehrbuch des Schuldrechts*, 1st vol., 14th ed., Verlag C. H. Beck, München (Munich).

Larenz, K and Canaris, CW (1994), *Lehrbuch des Schuldrechts*, 2nd vol., 2nd half-binding, 13th ed; Verlag C H Beck, München (Munich).

Larenz, K and Wolf, M (1997), *Allgemeiner Teil des Bürgerlichen Rechts*, 8th ed., Verlag C. H Beck, München (Munich).

Leier, Barbara, (2000), *Haftung der Zertifizierungstellen nach dem SigG - Betrachtung der geltenden und Überlegung zur zukünftigen Rechtslage*, Multimedia und Recht (MMR), 2000 (13).

Lockett, N and Egan, M (1995), *Unfair Terms in Consumer Agreements - The New Rules Explained*, John Wiley & Sons, Chichester, New York, Brisbane, Toronto, Singapore.

Lorenz, W (1994), *Contracts and Third-Party Rights in German and English Law,* in Markesinis, Basil S. (ed.) (1994), *The Gradual Convergence - Foreign Ideas, Foreign Influences and English Law on the Eve of the 21st Century*, Clarendon Press, Oxford.

Markesinis, B S (1994), *The German Law of Torts - A Comparative Introduction*, 3rd ed., Clarendon Press, Oxford.

Mason, Stephen, (1999/2000), *Electronic Signatures: The Technical and Legal*

Ramifications, 1999/2000 10 C & L 37.

Medicus, D (1999), *Bürgerliches Recht*, 18th ed. Carl Heymanns Verlag, Köln (Cologne), Berlin; Bonn and München (Munich).

Miller, C J (1998), Harvey, B W and Parry, D L (1998), *Consumer and Trading Law - Text, Cases and Materials*, Oxford University Press, Oxford.

Nicoll, C (2000), *Internet Regulations: Potential Liabilities*, Commercial Liability L. Rev. 2000 (1) 15.

Oughton, D and Lowry, J (2000), *Textbook on Consumer Law*, 2nd ed; Blackstone Publishing, London.

Rebel, T F and Koenig, W (1999), *Ensuring Security and Trust in Electronic Commerce* in Sudweeks, Fay and Romm, Celia T. (1999), *Doing Business on the Internet - Opportunities and Pitfalls*, Springer Verlag, London, Berlin, Heidelberg, 101.

Reed, C (2000a), *Internet Law: Text and Materials*, Butterworths, London, Edinburgh, Dublin.

Reed, Christopher (2000b), *What is a Signature?*, Journal of Information, Law & Technology (JILT) 2000 (3) <http://elj.warwick.ac.uk/jilt/00-3/reed.html>.

Rogers, W V H (1994), *Winfield and Jolowicz on Tort*, 14th ed; Sweet & Meaxwell, London.

Roßnagel, A (1998), *Das Gesetz und die Verordnung zur digitalen Signatur - Entstehung und Regelungsgehalt*, Recht der Datenverarbeitung (RDV), 1998 (5).

Sinisi, V (2001), *Digital Signature Legislation in Europe*, 2001, 16 BJIBFL 17.

Smedinghoff, T J (1998), *Certification Authority Liability Analysis*, American Bankers Association, Washington D C.

The Economist (2000), *SURVEY: GOVERNMENT AND THE INTERNET - Handle with Care*, 22. June 2000.

Thomas, (?) *Palandt*, [Details to be advised].

Timm, B (1997), *Signaturgesetz und Haftungsrecht*, Datenschutz und Datensicherheit (DuD) 1997 (21), 52.

Treitel, G H (1999), *The Law of Contract*, 10th ed; Sweet & Maxwell, London.

Uwer, H (2000), *Kostendruck fördert eGovernment*, Frankfurter Allgemeine Zeitung, FAZ.net, 28. November 2000, <http://www.faz.net/IN/INtemplates/faznet/default.asp?

tpl=uptoday/content.asp&doc={ABFED30B-E817-437F-ADCC-99E88CB70C0E}&rub={9E7BDE6C-469E-11D4-AE7B-0008C7F31E1E}>.

Van Gerven, W (ed.), Lever, J, Larouche, P, von Bar, C, Viney, G (1999), *Cases, Materials, and Text on National, Supranational and International Tort Law - Scope of Protection*, Hart Publishing, Oxford.

von Bar, C (1994), *Liability for Information and Opinions causing pure economic Loss to Third Parties: A Comparison of English and German Case Law*, in Markesinis, B S (ed.) (1994), *The Gradual Convergence - Foreign Ideas, Foreign Influences and English Law on the Eve of the 21st Century*, Clarendon Press, Oxford.

von Bar, C (1998), *Verträge mit Schutzwirkung zugunsten Dritter, Drittschadensliquidation and extension of duty of care*, 5, in The Institute of Comparative Law (Chuo University) (ed.) (1998), *Toward Comparative Law in the 21st Century - The 50th anniversary of The Institute of Comparative Law in Japan Chuo University*, Chuo University Press, Tokyo.

Youngs, R (1994), *Sourcebook on German Law*, Cavendish Publishing, London and Sydney.

Zweigert, Konrad and Kötz, Hein (1998), *An Introduction to Comparative Law*, 3rd ed., Clarendon Press, Oxford

Table of Cases

England and Wales

Al Nakib Investments (Jersey) Ltd. v. Longcroft [1990] 1 W. L. R. 1390.

Amherst v. James Walker Goldsmith and Silversmith Ltd. [1983] Ch. 305.

Bagot v. Stevens, Scanlan & Co. Ltd. [1966] 1 Q. B.197.

Bowerman v. Association of British Travel Agents Ltd. [1995] N. L. J. 1815.

Brown v. Rolls-Royce Ltd. [1960] 1 W. L. R. 210.

Caparo Industries plc v. Dickman [1990] 2 A. C. 605.

Carlill v. Carbolic Smoke Ball Co. [1893] 1 Q. B. 256.

Cie. Française d'Importation, etc., S. A. v. Deutsche Continental Handelsgesellschaft [1985] 2 Lloyd's Rep. 592.

Clark v. Kirby-Smith [1964] Ch. 506.

Collen v. Wright (1857) 8 E. & B. 647.

Currie v. Misa (1875) L. R. 10 Ex. 153.

First Energy (UK) Ltd v. Hungarian International Bank Ltd [1993] 2 Lloyd's Rep. 195.

Hadley v. Baxendale (1854) 9 Ex. 341.

Hedley Byrne & Co. Ltd. v. Heller & Partners Ltd. [1964] A. C. 465.

Henderson v. Merrett Syndicates Limited [1995] A. C. 145.

Howard Marine v. Odgen [1978] Q. B. 574.

Ignazio Messina & Co. v. Polskie Linie Oceaniczne [1995] 2 Lloyd's Rep. 566.

Mansukhani v. Sharkey [1992] 2 E. G. L. R. 105.

Interfoto Picture Library Ltd. v. Stiletto Visual Programmes Ltd. [1988] 1 All. E. R. 348.

James McNaughton Papers Group Ltd. v. Hicks Anderson & Co. [1991] All. E. R. 134.

Koufos v. Czarnikow Ltd. [1969] 1 A. C. 350.

Liesbosch Dredger v. SS Edison [1933] A. C. 449.

New Zealand Shipping Co. Ltd. v. A. M. Satterthwaite & Co. Ltd. [1975] A. C. 154
(also known as *The Eurymedon*).

O'Connor v. Kirby [1972] 1 Q. B. 90.

Olley v. Marlborough Court [1949] 1 All. E. R. 127.

Osman v. UK (1998) 5 B. H. R. C. 293.

Pan Atlantic Insurance Co. Ltd. v. Pine Top Insurance Co. Ltd. [1995] 1 A. C. 501, 542.

Photo Production Ltd. v. Securicor Transport Ltd. [1980] A. C. 827.

Robinson v. Harman (1848) 1 Ex. 850.

Smith v Eric S. Bush [1990] 1 A. C. 831.

The Agrable [1987] 2 Lloyd's Rep. 223.

The Amazonia [1990] 1 Lloyd's Rep. 238.

The Antclizo [1987] 2 Lloyd's Rep. 130.

The Golden Bear [1987] 1 Lloyd's Rep. 330.

The Hannah Blumenthal [1983] 1 A. C. 854.

The Leonidas D [1985] 1 W. L. R. 925.

The Maritime Winner [1989] 2 Lloyd's Rep. 506.

The Multibank Holsatia [1988] 2 Lloyd's Rep. 486.

Trumpet Software Pty Ltd. v. OzEmail Pty Ltd. [1996] 34 I. P. R. 481.

Thornton v. Shoe Lane Parking [1971] 2 Q. B. 163.

White v. Jones [1995] 2 A. C. 207.

'Wagon Mount' Overseas Tankship (UK) Ltd. v Morts Dock & Engineering Co. [1961] A. C. 388.

USA

Ultramares Corporation v. Touche Niven & Co. (1931) 255 NY 170 (Cardozo J.).

Germany

Reichsgericht, *Official Series (Civil Matters)*, **vol. 78**, 108.

Reichsgericht, *Official Series (Civil Matters)*, **vol. 127**, 222.

BGH, *Official Series (Civil Matters)*, **vol. 4**, 2.

BGH, *Official Series (Civil matters)*, **vol. 49**, 354.

BGH, *Official Series (Civil Matters)*, **vol. 51**, 96.

BGH, *Official Series (Civil Matters)*, **vol. 56**, 274.

BGH, *Official Series (Civil Matters)*, **vol. 56**, 273.

BGH, *Official Series (Civil Matters)*, **vol. 70**, 329.

BGH, *Official Series (Civil Matters)*, **vol. 100**, 117.

BGH, *Official Series (Civil Matters)*, **vol. 127**, 378.

BGH, *Official Series (Civil Matters)*, **vol. 128**, 168.

BGH, *Official Series (Civil Matters)*, **vol. 129**, 168.

BGH, *Official Series (Civil Matters)*, **vol. 133**, 42.

BGH *Wertpapiermitteilungen -Zeitschrift für Wirtschafts- und Bankrecht (WM)* **1956** 1229.

BGH *Neue Juristische Wochenschrift (NJW)* **1968**, 1929.

BGH *NJW* **1973**, 322.

BGH *NJW* **1976**, 1844.

BGH *NJW* **1983**, 1053.

BGH *NJW* **1984,** 355.

BGH *NJW* **1984,** 355.

BGH *NJW* **1985**, 489.

BGH *Juristen-Zeitung (JZ)* **1985**, 951.

BGH *Versicherungsrecht (VersR)* **1986**, 35.

BGH *NJW* **1987**, 1760.

BGH *NJW* **1989**, 2882.

BGH *NJW* **1991**, 32.

BGH *NJW* **1992**, 2080.

BGH *NJW* **1995,** 392.

Table of Legislation

European Community

Directive 1993/13/EC on unfair terms in consumer contracts.

Directive 1999/93/EC on a Community framework for electronic signatures (ESD).

England and Wales

Contracts (Rights of Third Parties) Act 1999.

Electronic Communications Act 2000.

Unfair Terms in Consumer Contracts Regulations 1994 (UTCCR).

Uniform Contract Terms Act 1977 (UCTA).

Germany

Act for a Basic Framework for Electronic Signatures 2001 *(Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgsetz (SigG)))* and respective Ordinance.

Civil Code *(Bürgerliches Gesetzbuch (BGB)).*

Criminal Code *(Strafgesetzbuch (StGB)).*

Digital Signature Act 1997 *(Signaturgesetz).*

Italy

Italian legislation (DPR of 10. November 1997, no. 513).

Appendix

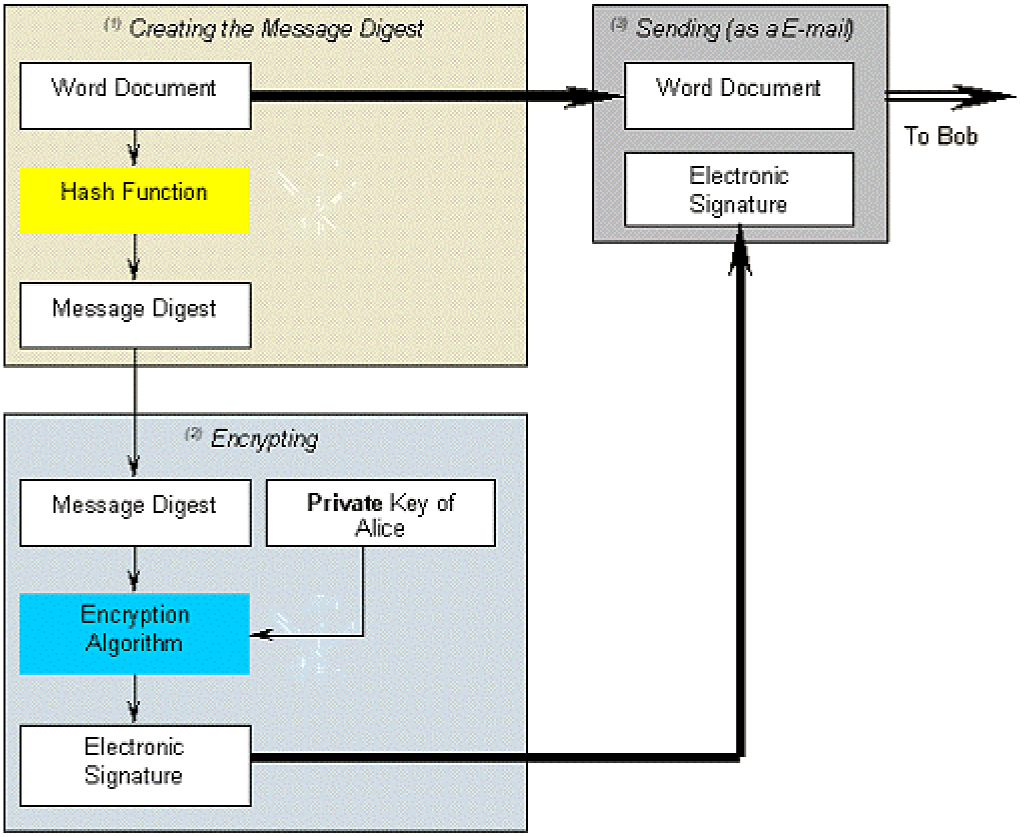


Figure 1: Sending an Electronically Signed Document

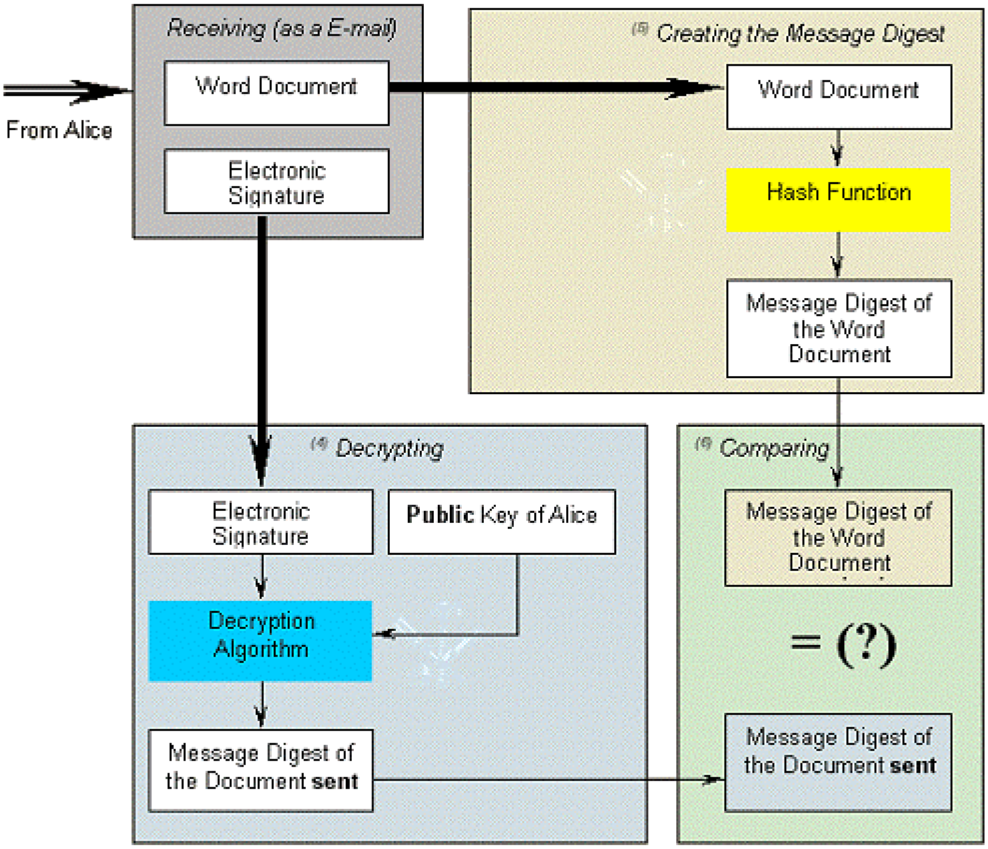


Figure 2: Validating an Electronically Signed Document

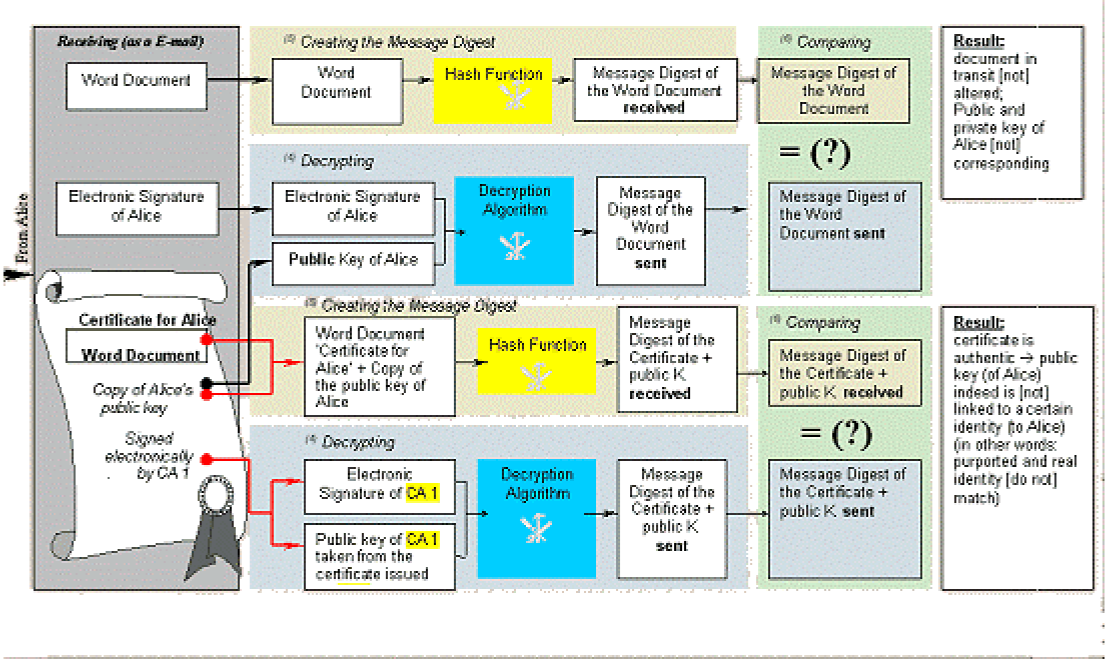
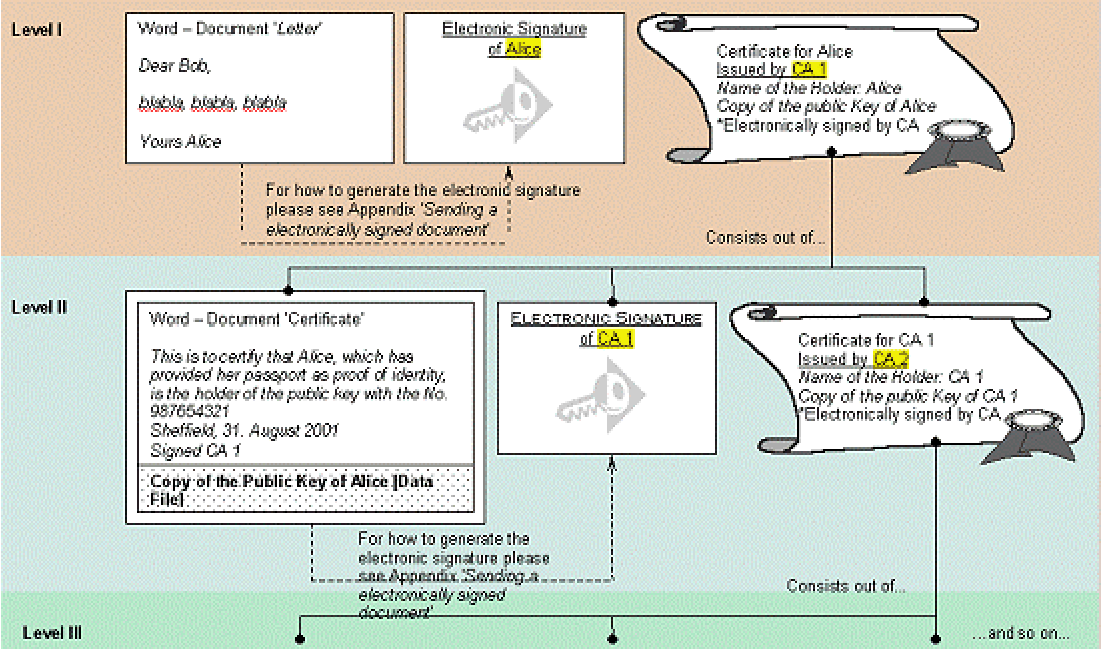

Receiving (as a E-mail)
Word Document
Electronic Signature of Alice
From Alice
Certificate for Alice
Word Document
Copy of Alice's public key
Signed electronically by CA 1
(5) Creating the Message Digest
Word Document
Hash Function
Message Digest of the Word Document received
(4) Decrypting
Electronic Signature of Alice
Public Key of Alice
Decryption Algorithm
Message Digest of the Word Document sent
(6) Comparing
Message Digest of the Word Document
= (?)
Message Digest of the Word Document sent
Result:
document in transit [not] altered;
Public and private key of Alice [not] corresponding
(5) Creating the Message Digest
Word Document 'Certificate for Alice' + Copy of the public key of Alice
Hash Function
Message Digest of the Certificate + public K received
(4) Decrypting
Electronic Signature of CA 1
Public key of CA 1 taken from the certificate issued
Decryption Algorithm
Message Digest of the Certificate + public K sent
(6) Comparing
Message Digest of the Certificate + public K received
= (?)
Message Digest of the Certificate + public K sent
Result:
certificate is authentic → public key (of Alice) indeed is [not] linked to a certain identity (to Alice) (in other words: purported and real identity [do not] match)

Figure 3: Validating an Electronically Signed Document with Certificate



Word – Document '*Letter*'

Dear Bob,

blabla, blabla, blabla

Yours Alice

Certificate for Alice
Issued by CA 1
Name of the Holder: Alice
Copy of the public Key of Alice
*Electronically signed by CA

For how to generate the electronic signature please see Appendix '*Sending a electronically signed document*'

Word – Document 'Certificate'

This is to certify that Alice, which has provided her passport as proof of identity, is the holder of the public key with the No. 987654321
Sheffield, 31. August 2001
Signed CA 1

Copy of the Public Key of Alice [Data File]

Certificate for CA 1
Issued by CA 2
Name of the Holder: CA 1
Copy of the public Key of CA 1
*Electronically signed by CA

For how to generate the electronic signature please see Appendix '*Sending a electronically signed document*'

Figure 4: Certification Structure

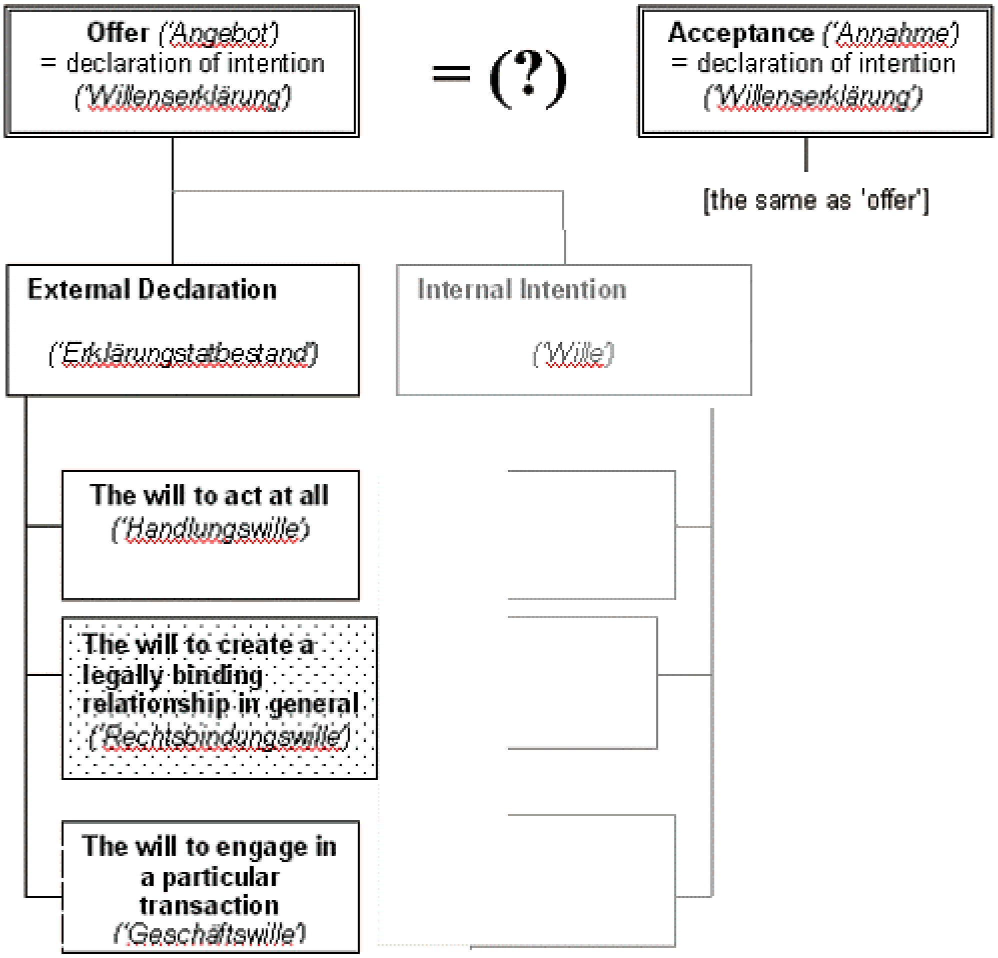
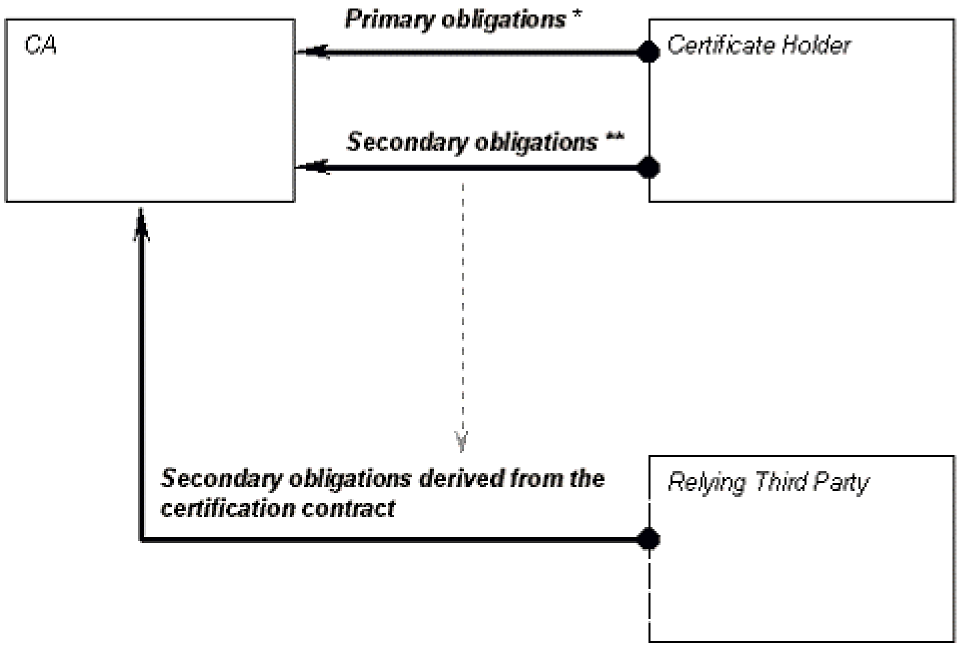


Figure 5: Contract in German Civil Law



* e. g. providing accurate information in the certificate issued, maintaining the certificate revocation list, etc.

** i. e. to take due care while performing the primary obligations

Figure 6: Contract with a Protective Effect Towards a Third Party
('Vertrag mit Schutzwirkung zugunsten Dritter')

Glossary of CA Specific Terms

advanced electronic signatures (EC Directive term)	- will have the same value as a hand written signature and be admissible as evidence in legal proceedings - is based on a qualified certificate and is created by a secure signature creation device
certification authority (CA)	- also certification-service-provider (term used in the EC Directive 1999/93) - is a body, either public or private, that seeks to fill the need for trusted third party services in electronic commerce by issuing digital certificates that attest to some fact about the subject of the certificate
Certification Practice Statement (CPS)	- defines the representations CAs make and warranties they hold out in respect of certificates
certification-service-provider (EC Directive term)	- see *certification authority*
certificate	- means an electronic attestation which links a public key to a person and confirms the identity or other attributes - see also *qualified certificate*
certificate revocation list	- since personal circumstances change and the reality represented by the certificate is out of date, certificates have limited periods of validity or are subject to periodic re-confirmation by the CA. Certificates which are outdated or have been compromised, e. g. by disclosing the private key, are listed in this list which is maintained by the issuing CA - when, for example,

the relying party is suspicious about the validity of the certificate, he interrogates the CA’s Certificate Revocation List

‘***d***igest’ function	- see *‘hash’ function*
electronic signature *(in a technical sense)*	- also called ‘ciphertext’ - is the result of the

encryption of the message digest with the private key (Encryption is carried out by performing a series of mathematical functions (an encryption algorithm) which has two inputs: the ‘message digest’ which is nothing more than a string of 1s and 0s and the private key which is itself a number) producing a series of different numbers

‘***h***ash’ function	- also ‘digest’ function - is an algorithm which

creates a digital representation or ‘fingerprint’ in form of a ‘hash value’ or ‘hash result’ or message digest of a standard length which is usually much smaller than the message but nevertheless substantially unique to it. Any change to the message invariably produces a different hash result when the same hash function is used. In the case of a secure hash function it is ‘computationally infeasible’ to derive the original message from knowledge of its ‘hash value’.

hash result	- see *message digest* - also hash value
hash value	- see *message digest* - also hash result
message digest	- also ‘hash value’ or ‘hash result’ - a digital

representation or ‘fingerprint’ of a standard length which is usually much smaller than the message but nevertheless substantially unique to it. Any change to the message invariably produces a different hash result when the same hash function is used.

‘***n***on-qualified’ certificate	- see *certificate*
‘***p***ublic key cryptography’	- uses two different but mathematically related

keys, each of which will decrypt documents encrypted by the other key. One key, chosen arbitrarily, is used to transform data into a seemingly unintelligible form and is kept secret, while the other is made public. All effective electronic signatures require the use of a 'one-way function’ (irreversibility). This means that if a document, signed electronically by Alice with her private key, is sent to Bob, Bob must be able to decrypt the document’s signature element with the help of Alice’s public key, but must not be able to re-encrypt it with this key. In other words it must be ‘computationally infeasible’ to derive the private key from the knowledge of the public key. Otherwise the discovered private key could be used to forge digital signatures of the holder.

qualified certificate (EC Directive term)	- the requirements for an qualified certificate (Art.

2 Nr.10 ESD) are set out in Annex I and II of the ESD: Qualified certificates must contain: *‘(a) an indication that the certificate is issued as a qualified certificate; (b) the identification of the certification-service-provider and the State in which it is established; (c) the name of the signatory or a pseudonym, which shall be identified as such; (d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended; (e) signature-verification data which correspond to signature-creation data under the control of the signatory; (f) an indication of the beginning and end of the period of validity of the certificate; (g) the identity code of the certificate; (h) the advanced electronic signature of the certification-service-provider issuing it; (i) limitations on the scope of use of the certificate, if applicable; and (j) limits on the value of transactions for which the certificate can be used, if applicable.’* - Certification-service-provider issuing qualified certificates must meet the following requirements: They must: *‘(a) demonstrate the reliability necessary for providing certification services; (b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service; (c) ensure that the date and time when a certificate is issued or revoked can be determined precisely; (d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued; (e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards; (f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them; (g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data; (h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance; (i) record all relevant information concerning a qualified certificate*

for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically; (j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services; (k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate; (l) use trustworthy systems to store certificates in a verifiable form so that: - only authorised persons can make entries and changes, - information can be checked for authenticity, - certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and - any technical changes compromising these security requirements are apparent to the operator.’

‘***r***egular’ electronic signature (EC Directive term) - *‘means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication’* (Art. 2 Nr. 1 ESD) - may, at least, not be denied legal effectiveness and admissibility as evidence on the grounds that it is in electronic form, or not based upon a qualified certificate, or not based upon a qualified certificate issued by an accredited certification-service-provider, or not created by a secure signature-creation device (Art. 5 (2) ESD)

Relying Third Party Charter - defines the representations CAs make and warranties they hold out in respect of certificates

secure signature creation device (EC Directive term) - the requirements for secure signature-creation devices are set out in Annex III of the ESD: *‘1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that: (a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured; (b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology; (c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others. 2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.’*