Electronic signatures in German, French and Polish law perspective

DR CHRISTIANE BIEREKOVEN, PHILIP BAZIN AND TOMASZ KOZLOWSKI

This article presents some significant issues on the recognition of electronic signatures with regard to foreign certificates from the perspective of German, French and Polish law. The European Union legislation applies to Germany and France, and has served as a guide for Polish legislation in the course of preparations of the accession of Poland to the European Union. There are therefore strong similarities between the legislation of these countries, but as the French example shows, the results may also differ with regard to the material law applicable to a contract. The difference between simple and advanced electronic signature is discussed within the context of French law.

This article elaborates on conditions of recognition of electronic signatures and the relevance of such recognition for the legal systems of the Germany, France and Poland. It seems that the Electronic Signature Directive has been successfully implemented, and provides for clear recognition criteria within the European Union. The recognition of certificates from third countries depends on the fulfillment of the criteria set out in the Directive. The Polish law provides for a special position of European Union based suppliers of certificates in terms of their recognition.

Electronic Signatures in Germany

■ European background

The European Directive on Electronic Signatures[1] binds the German legislator. Thus, the requirements for electronic signatures laid down in this Directive apply to the German legislation on electronic signatures.

It may be stressed that Germany was the first country in the European Union that issued a law on electronic, respectively digital, signatures prior to the Electronic Signature Directive. The Act on Digital Signatures came into force on 1 August 1997 and was restricted to the use of digital signatures only. It had to be amended after the Electronic Signature Directive was published, because the Directive provides for electronic signatures in general and is not restricted to the use of digital signatures only.

■ The German legislation

The Electronic Signature Directive was implemented into German law by the "Act on outlining Conditions for Electronic Signatures and for the Amendment of further Regulations" (Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften), hereinafter referred to as "SigG" - of 21 May 2001. It came into force on 22 May 2001. It replaces the former Act on Digital Signatures (Verordnung zur digitalen Signatur No: Signaturgesetz).

Art. 23 SigG provides for the recognition of foreign electronic signatures and products for electronic signatures. It distinguishes between electronic signatures originating in EU member states, states of the European Free Trade Association (EFTA) and electronic signatures originating in third countries.

■ Electronic Signatures originating in a Member State of the EU or the EFTA

According to Art. 23 § 1 SigG electronic signatures, which are based on a qualified certificate of a member state of the EU or the EFTA, are recognized as legally equivalent to qualified electronic signatures in the sense of the SigG, provided that those qualified certificates comply with the provisions of Art. 5 § 1 of the

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ 19.1.2000 L13/12).

If the certification body approves the security concept, the certification service provider is entitled to call itself "accredited certification service provider" and to rely on the approved security in the course of business and legal relations

Electronic Signature Directive.

This means that electronic signatures that are based on qualified certificates of member states of either the EU or the EFTA that comply with the provisions of Art. 5 § 1 of the Electronic Signature Directive are recognized as legally equivalent with qualified electronic signatures in the sense of the SigG. So, the requirements for the recognition may be determined by Art. 5 § 1 Electronic Signature Directive.

■ Electronic Signatures originating in a Third Country

Regarding the recognition of electronic signatures originating in third countries, Art. 23 § 1 SigG implements the provisions of Art. 7 § 1 of the Electronic Signature Directive and further requires that the certificate in the sense of Art. 7 § is to be used for an electronic signature in the sense of Art. 5 § 1 Electronic Signature Directive. An electronic signature in the sense of Art. 5(1) is an advanced electronic signature which is based on a qualified certificate and is created by a secure –signature-creation device. Pursuant to Art. 2 No. 1 an "advanced electronic signature" is an electronic signature which is uniquely linked to the signatory, is capable of identifying the signatory, is created using means that the signatory can maintain under his sole control and eventually is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. A "qualified certificate" is a certificate that meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfills the requirements laid down in Annex II[2], Art. 2 No. 10. A "secure-signature-creation" device is a signature-creation device that meets the requirements laid down in Annex III[3]. Hence, if an electronic signature originating in a third country is an advanced electronic signature in the sense of Art. 2 No. 2 Electronic Signature Directive as outlined before it has to be recognized as legally equivalent to qualified electronic signatures in the sense of the SigG.

■ Note

The German SigG provides for voluntary accreditation in Art. 15. This means that a certification service provider may apply for an accreditation with the relevant official authorities. It has to comply with further requirements of the SigG. This means that such certification service provider has to present a security concept in the sense of Art. 4 § 3 in which it shows that it meets the requirements of both the SigG and the Signaturverordnung (Regulations on Electronic Signatures), Art. 15 § 1 SigG. This security concept has to be approved by a certification body ("Bestätigungsstelle"), Art. 15 § 2 SigG. If the certification body approves the security concept, the certification service provider is entitled to call itself "accredited certification service provider" and to rely on the approved security in the course of business and legal relations.

Pursuant to Art. 23 § 2 SigG electronic signatures in the sense of § 1 are recognized as legally equivalent to qualified electronic signatures based on a certificate of an accredited certification service provider in the sense of Art. 15 § 1 SigG if it has been demonstrated that they adhere to the same security standard. This means that electronic signatures originating in the member states of the EU or the EFTA or in third countries and which comply with the requirements of Art. 23 § 1 SigG have to show the security standard being applicable to electronic signatures based on a certificate of an accredited certification service provider. If this is proven, they are recognized as legally equivalent to electronic signatures based on a certificate of an accredited certification service provider in the sense of Art. 15 § 1 SigG and may, therefore, be promoted as electronic signatures based on a certificate of an accredited certification service provider. Obtaining approved statues means the accredited certification service provider can promote this in the course of business and rely on the legal effect in its relations with its customers.

■ Products for electronic signatures

Products for electronic signatures originating in either a member state of the EU or the EFTA which comply with the provisions of the Electronic Signature Directive and which have been officially approved, are recognized in Germany. This means that those products for electronic signatures which have been tested in one of the member states of the EU or the EFTA and which have been officially approved to comply with the requirements of the Electronic Signature Directive are recognized in Germany.

It may be stressed that the definition of "products for electronic signatures" in Art. 2 No. 13 SigG:

[2] The Annexes I and II are attached to the Electronic Signature Directive 1999/93/EC, of 19.01.2000, L 13/18, L13/19.
[3] Annex III is attached to the Electronic Signature Directive, L13/20.

"Produkte für elektronische Signaturen" sichere Signaturerstellungseinheiten, Signaturanwendungskomponenten und technische Komponenten für Zertifizierungsdienste	"Products for qualified electronic signatures" shall be secure signature-creation devices, signature-application components, and technical components for certification services;

is not identical with the definition of "electronic-signature product" in Art. 2(12) of the Electronic Signature Directive:

> 'electronic-signature product' means hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;

According to Art. 2 No. 10 SigG, a secure signature-creation device means components of hardware or software which are intended to either store or use the signature key. Those components have to meet the requirements of Art. 17 or 23 SigG and the relevant stipulations of the Regulations on electronic signatures, and are intended to be used for qualified electronic signatures. Thus, in contrast to the definition of "products for electronic signatures" in the sense of Art. 2(12) of the Electronic Signature Directive, the definition of "products for electronic signatures" in Art. 2 No. 13 SigG also includes the use of the respective signature key. Furthermore, a "signature-application component" means hardware or software products that are intended (a) to be used for the process of the creation or the verification of a qualified electronic signature or (b) to verify a qualified electronic signature or a qualified certificate and to show the results of such verification. These requirements are partly included in the definition of a "signature-verification device" of Art. 2(8) of the Electronic Signature Directive and partly in the definition of "electronic-signature product" of Art. 2(12) of the Electronic Signature Directive. The most important difference between the two definitions is that the definition of Art. 2 No. 10 SigG also includes the use of the signature key whereas the definition of Art. 2(12) of the Electronic Signature Directive does not.

■ Relevance of the Recognition

It has to be pointed out that under German law, the use of qualified electronic signatures in the sense of the SigG amongst other things has at least two important consequences. First, pursuant to Art. 126a of the German Civil Code, qualified electronic signatures in the sense of the SigG are to be recognized as legally equivalent to handwritten signatures.

Secondly, according to Art. 292a of the German Code of Civil Procedure, it is presumed that an electronic declaration that has been signed with a qualified electronic signature in the sense of Art. 126a of the German Civil Code is an authentic declaration of the signature-holder. Thus, in a litigation the party who contests the authenticity of the electronic declaration of the other party has to present facts that cause reasonable doubts that the declaration in question has been made willingly by the signature-holder.

Consequently, if an electronic signature originating in a member state of the EU or the EFTA or a third country is recognized as legally equivalent to qualified electronic signatures in the sense of the SigG, it may comply with the requirements of a handwritten signature, and the signature-holder may rely on the presumption provided for by Art. 292a German Code of Civil Procedure. So, if the opponent contests the authenticity of the electronic declaration that has been signed with an electronic signature originating in a third country that is recognized legally equivalent to a qualified electronic signature in the sense of Art. 126a of the German Civil Code, the opponent has to present facts that cause reasonable doubts that this declaration has been made willingly by the signature-holder.

By contrast, if the electronic signature originating in a third country is not recognized as legally equivalent to a qualified electronic signature in the sense of Art. 126a of the German Civil Code, the signature-holder has to prove that the declaration in question has been made willingly by him. In that case, the signature-holder has to present witnesses who may testify accordingly, which in fact means that he may only sign electronically in the presence of a witness. In practice, it is assumed that this will rarely happen, since documents in general are signed alone and so are or will be electronic documents. Therefore, it may be of great advantage for the signature-holder if his electronic signature is recognized legally equivalent to qualified electronic signatures in the sense of Art. 126a German Civil Code.

Electronic Signatures in France

■ A paradoxical question

The French view on the electronic signatures recognition problems focuses on a slightly different issue. From the French law perspective in the EU context, the crucial question is: it is possible for one EU jurisdiction or a competent court to recognize the validity of a certified signature, and another one to refuse such recognition. The question so formulated seems to be paradoxical.

The Electronic Signature Directive lays down a strong principle of free circulation of electronic-signature products and their functional equivalence. This principle refers to the general principle of free movement of goods and services that governs trade within the Common Market. The Electronic Signature Directive lays down principles of compatibility and interoperability of electronic-signature products on the level of the Member States, as set out in the fifth recital of the Preamble:

> The interoperability of electronic-signature products should be promoted; in accordance with the article 14 of the Treaty

What is true for every state should certainly apply to every court proceedings conducted by competent courts. Bearing in mind what has been said above, it would have been contradictory for the European legislation on electronic signatures if the same certificate of signature was considered differently in different proceedings. However, a more detailed analysis provides for a more sophisticated answer.

The following should be taken into account: the scope of application of the electronic signature as defined by the Directive and the two categories of the signatures established by the Directive.

■ The scope of application of electronic signatures as defined by the Directive: contracts subject to the formal requirements

Article 1 of the Directive defines the scope of applicability in a rather general manner. It provides that:

> The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition … [and]… establishes a legal framework for electronic signatures

Notwithstanding the foregoing, the Electronic Signature Directive is not applicable to all kinds of signatures. Article 1(2) provides for the following exclusion:

> It [the Directive] does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law

Hence the situation in which the signature by itself is not enough to conclude a contract or assume an obligation is excluded from the scope of applicability of the Directive. Such is the case in French law where different sorts of contracts require observance of the "written" form and, if such is missing, the observance of certain formalities. For example, insurance contracts, marriage contracts or articles of association should be completed in writing, whereas a contract of marriage should be carried out before a notary. In such a case, no matter what means of electronic signature were used, it would not be enough to give the act in question legal effect. It is because the law requires that also other formalities must be observed.

This allows us to understand the different position that may be taken by different courts with regard to same signature tool. If certain signature tools are used in cases where other formalities are also required, whether the particular signature tool was in conformity with the requirements of the Directive would not be decisive. Within the requirements of national law, the use of such a signature is not enough to create an act that requires other conditions to be fulfilled.

Consider the contract of insurance as an example. Assume the insured faces a claim from a third party- victim of an accident. The insured seeks to call upon the guarantee of the insuring entity. In such a case, French law requires the insured to prove the two following aspects:

- The existence of the contract.
- The obligation to provide a guarantee.

The law also requires the contract of insurance to be completed in "writing" which means, in the present wording of the Civil Code, to use paper form. It means that the existence of a contract is only possible if it is in paper form. The case may be that the insured is only in the possession of an electronic copy of the contract. Such an electronic copy, even if signed, would not be enough to be regarded as a proof, because the law requires that the contract in its entirety should exist on paper. In such a case the judge may disregard the electronic signature, even if its validity was not in question.

On the other hand, consider the same example of the insurance contract but where it has been produced on paper, and where the annex has been signed electronically. If the condition with regard to the existence of the contract was

What is true for every state should certainly apply to every court proceedings conducted by competent courts

satisfied (execution of the contract in paper form) the proof with regard to the annex (which is not submitted by law to the same requirements of the paper form) may be carried out using an electronic signature.

In summary, the requirements as to the form constitute the first explanation of the possibility of a different approach of two jurisdictions to the same form of electronic signature that may have been used. However, the same difference may also appear in a different scenario. It is the case where two signatures are used in conformity with the Directive, but have different evidential value. The Directive utilizes the distinction between two categories of electronic signature.

■ The two categories of signature used by the Directive

The Directive, in article1, refers to a "framework for electronic signatures". The plural used in that phrase does not simply refer to the signatures that exist in every member state. It refers to the two categories of signatures introduced by the Directive. Those two categories may be characterized in the following way:

- The "simple" electronic signature which is only destined as authentication (to guarantee identity) of the author of a message, and which is only a method of authentication.
- The "advanced" electronic signature which guarantees identity and integrity of a message and which, taking into account stringent conditions of its delivery, is destined to have the same legal value as the hand written signature

These are in fact two different forms of electronic signatures which do not have the same legal value and which result from two different cultures.

■ The Roman culture of the identity card

If a person affixes their signature on a document, they may have to justify the validity of that signature to a third party. Two questions arise: Is the natural person who signs the person who he purports to be? And how should it be proved?

In the Roman legal system, the answer is simple: proof is adduced by producing an identity card. The official document is issued by the public authority on the base of other official documents. In France, it is an excerpt from the act of birth. The National Identity Card contains the official master of the hand signature. Indeed, as the National Identity Card is delivered by Civil Servants in France, the National Identity Card is considered to be the strongest tool to prove the identity, nationality and signature of a person.

It is this master signature which serves as element of comparison and, consequently of authentication in case of a dispute. To 'authenticate' in the etymology of the word means to verify the author of a message. The best method to establish a connection between the message and its author and consequently its uniqueness, it is to establish a physical connection between the person and the tool they are using. If I sign using my own hand, I confirm the uniqueness of my signature with regard to the others because my hand by very definition is unique.

But the uniqueness resulting from the physical connection between the tool (the hand) and the visible result of the tool (the signature) makes the hand signature something more than just the method of identification. It goes much further because it is directly connected to a person and therefore it also manifests the will. To sign with a hand is not only to simply identify oneself, but it is also to manifest the consent to a legal act. To sign with a hand means to show consent and will to create obligations. Therefore the legal value of the signature refers to its official aspect (the master of signature being deposited with the public authority) and its physical connection with the person whose consent is manifested. Compared with the common law, the signature always serves to identify the signatory of a contract and to acknowledge consent to a legal act, unless the contractor gives the order to a third person to contract for him and under his name.

■ The Anglo-Saxon culture of authentication

Our English friends ignore the mechanism of identity card that constitutes strong reference in terms of a proof. They are much more familiar with "methods of authentication" which are practically the contractual procedures by which two persons define the specific signs by which they would be mutually recognizable. This is the culture of "authentication" that takes different forms, such as the use of a password, access code, chip card or USB key. These methods are often used in private or semi-private networks, like a safe guarded intranet.

This method of proceeding has a direct influence on the understanding of electronic signature. Very simply one could say that the signature being a "method of the authentication" for some, would be the "identity" and "consent" for the others. However, those two forms are not subject to the same technical requirements.

To sign with a hand is not only to simply identify oneself, but it is also to manifest the consent to a legal act

■ The simplicity of electronic signature understood as a method of authentication

As already mentioned, the method of authentication may take very different forms. Especially, it may be used under a covenant with regard to methods of evidence. I decide that in my relations with the bank I will identify myself by a code composed of four digits. I decide that in my relations with my suppliers I will identify myself by a password to obtain access to a private network. I decide that in relations with my clients, I will be identified by a combination of password, a chip card or USB key on which the data generated by me for my identification is installed.

In short, an electronic signature as understood as a method of authentication within the meaning of the Directive, is simple to produce and simple to function. But what is its value in terms of proof?

Between the parties of the agreement it is certainly strong. But this value is only a relative one, because it does not apply to other parties. These authentication tools only have a legal value in relation to those who voluntary accept to be bound by them. For the third parties, those methods are without any effect. A signature should be effective against everyone, just like a hand written one. What makes the value of the advanced electronic signature it is its complexity.

■ The complexity of advanced electronic signature understood as a tool of identification and consent

From a legal point of view, the advanced electronic signature guaranties the integrity of a message and identity of its author. The tools that are used to produce it (qualified certificates) are delivered observing stringent conditions. Notably, the provider of certification services should assure by physical contact, the existence and the identity of a given person or legal entity. Secondly, the certificate should be produced with the technology that responds to the stringent technical requirements, guaranteeing the holder of such a certificate against all risk of duplicating such a certificate. Finally, the provider of the certification services should present the special guaranties of competence and organization to obtain the right to issue the certificates characterized as "qualified".

To sum up, the advanced electronic signature does not have much to do with the simple method of authentication, which is the simple signature.

■ Different kinds of signatures

As there are two categories of signature, it is understandable why two jurisdictions or competent courts may have different opinions in relation to the same form of signature. The advanced electronic signature presents a much stronger guarantee in comparison to those offered by a simple signature. Because of this, and depending on the circumstances of the case, it may well be the case that a simple electronic signature would be considered as valid in some circumstances and not in others.

For example if I order a CD over the internet and I use a simple electronic signature, it is possible that in case of a dispute the judge would consider a simple electronic signature as a valid proof with regard to the limited importance of the interests at stake. Quite the opposite, if I use the same signature to buy a car or jewellery, the judge would understandably take much more sceptical approach, and would consider the obligations to be of such importance that a simple signature would not suffice as the proof of those obligations.

In short, the simple electronic signature bears too great a risk of fraudulent usage to be given the same value in terms of proof as the advanced electronic signature.

■ Summary

The answer to the question under French law may be concluded as follows. It is possible that the same certificate of signature would be considered as a valid by one judge and not by another. This possibility of the different appreciation results from the distinctions in the European law between two categories of the signature. The "simple" electronic signature does not contain strong legal guaranties. The advanced electronic signature, on the other hand, presents important legal guaranties. Those guaranties are at least the same as those of a hand written signature. If a simple electronic signature is used for obligations of a limited importance, the judge may take a more generous approach to its usage.

Once it is used for obligations of substantial importance, the judge would take a more critical approach and consider only the advanced electronic signature as a valid proof that is acceptable in the court proceedings.

Electronic Signature in Poland

The Polish Act on Electronic Signature, dated 18.09.2001 (Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym), aimed to achieve similar standards as in the Electronic Signature Directive. The act on electronic signatures differentiates three kinds of signatures:

- electronic signature (Art. 3 item 1 of the Act),
- safe electronic signature (Art. 3 item 2 of the Act),
- safe electronic signature verified by qualified certificate (Art. 5 section 1 of the Act)

The last type of signature (safe electronic signature verified by qualified certificate) is equivalent to the hand written signature in terms of its legal effects[4]. The qualified certificate may be issued only by qualified entity subject to stringent requirements defined in the Act (Articles 14-20 and Article 23).

The entities providing qualified certificate services are subject to enrolment to the registry of the qualified suppliers of certificate services. The registry is supervised by the Ministry of Economy[5].

■ Recognition of foreign certificates supporting electronic signatures

Article 4 of the Act on Electronic Signatures sets out the conditions relating to foreign certificates. For a foreign certificate to be recognized, one of the following criteria has to be met:

1. podmiotowi świadczącemu usługi certyfikacyjne, który wydał ten certyfikat, została udzielona akredytacja,
2. przewiduje to umowa międzynarodowa, której stroną jest Rzeczpospolita Polska, o wzajemnym uznaniu certyfikatów,
3. podmiot świadczący usługi certyfikacyjne, który wydał ten certyfikat,został wpisany do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
4. podmiot świadczący usługi certyfikacyjne, mający siedzibę na terytorium spólnoty Europejskiej spełniający wymogi ustawy, udzielił gwarancji za ten certyfikat,
5. certyfikat ten został uznany za kwalifikowany w drodze umowy międzynarodowej zawartej pomiędzy Wspólnotą Europejską a państwami trzecimi lub organizacjami międzynarodowymi,
6. podmiot świadczący usługi certyfikacyjne, który wydał ten certyfikat, został uznany w drodze umowy międzynarodowej zawartej pomiędzy Wspólnotą Europejską a państwami trzecimi lub organizacjami międzynarodowymi.

1. The entity providing the certificate services has been entered to the register of the qualified entities providing certificate services.
2. The recognition is envisaged by an international convention on mutual recognition of the certificates to which Poland is party.
3. The provider of the certificate services fulfils the requirements of the Act and has been accredited in the Member State of European Union.
4. The provider of the certificate services with a seat in the European Union fulfilling the requirements of the Act has guarantied that certificate.
5. The certificate in question has been considered as qualified by an international convention concluded between European Union and third parties or international organisations.
6. The entity rendering certificate services which issued that certificate has been recognised by international convention concluded between the European Union and third parties or international organisations.

To sum up this discussion, the Polish Act on Electronic Signatures provides for the possibility of the recognition of electronic signatures produced with the certificates issued by entities in other countries, especially in member states of European Union. ■

[4] Article 5 section 2 reads: "Data in electronic format signed with safe electronic signature verified by valid qualified certificate are equivalent in their legal effects with documents signed by hand unless specific provisions of law provide otherwise."

[5] A list of entities rendering the certification services may be viewed on the web e.g. at http://www.centrast.pl/?i=10.

The Article is the result of work of the E-Commerce Group of Avrio Advocati, a European based legal network. The details of the network, the authors and their legal practices are available at www.avrio.net.

The discussion on German law is provided by Dr Christiane Bierekoven, Rechtsänwaltin, associate at Eimer Heuschmid Mehle, Germany, who specializes in unfair competition, intellectual property, trade marks, internet law, agency and distribution, International private law, European law. Dr Bierekoven won the Ehrhardt-Imelmann-Award 2001 of the University of Cologne.

bierekoven@avrio.net

The discussion on French law is provided by Philip Bazin Philip is an avocat at Barreau de Rouen, France, and a member of the Association pour le Développement pour l'Informatique Juridique and the Forum des Droits de l'Internet. His firm, Emo Herbert & Associes, is a member of the Association HSD, established by Ernst & Young.

pbazin@avoceha.com

The outline on Polish law is provided by Tomasz Kozlowski, of Radca Prawny (legal advisor), Poland, KRPiA Gluchowski Jedlinski Rodziewicz Zwara & Partners. Tomasz is a holder of Diplomas in EU, German, English and French Law from Universities in Cambridge (UK), Bonn (Germany) and Poitiers (DESS-France).

t.kozlowski@kpsc.com.pl