The Legal Classification of Identity-Based Signatures

Christoph Sorge
University of Paderborn
33098 Paderborn, Germany
christoph.sorge@uni-paderborn.de

Abstract

Identity-based cryptography has attracted attention in the cryptographic research community in recent years. Despite the importance of cryptographic schemes for applications in business and law, the legal implications of identity-based cryptography have not yet been discussed. We investigate how identity-based *signatures* fit into the legal framework. We focus on the European Signature Directive, but also take the UNCITRAL Model Law on Electronic Signatures into account. In contrast to previous assumptions, identity-based signature schemes can, in principle, be used even for qualified electronic signatures, which can replace handwritten signatures in the member states of the European Union. We derive requirements to be taken into account in the development of future identity-based signature schemes.

1 Introduction

Digital signatures are among the most widely used cryptographic schemes. A traditional cryptographic signature scheme allows anyone to create a key pair, consisting of a public key and a private key. The private key, which is to be kept secret, is used by the signatory to sign messages; signatures can be verified with the corresponding public key. Successful verification of a digital signature guarantees integrity and authenticity of the corresponding message. Non-repudiation is also achieved, i.e. it can be proven that the message was signed by the signatory. Only the public key, the message, and the signature are needed for this proof.

For digital signature schemes to become practical, a public key must be securely bound to the identity of its owner. Traditionally, Public Key Infrastructures (PKIs) have been used for this purpose. The core element of a PKI are so-called certification authorities (CAs)—also referred to as certification service providers (in the legal context). CAs certify the mapping between a public key and its owner by digitally signing a *certificate*, i.e. a data structure that contains both the identity and the public key. This way, if a CA is sufficiently trusted, users only need the CA's public key to verify the identity of any signatory who presents a certificate issued by that CA. The sender of a signed message can send the certificate along with the message itself (and the recipient must verify both the sender's signature and the certificate); under normal circumstances, this overhead is considered acceptable, but specific application scenarios may require a limitation of both message sizes and computational effort.

Digital signature schemes have proven useful, among others, for e-business and e-government. Legislation in many countries defines requirements for signatures of electronic documents (also called electronic signatures) to have legal effect (both to fulfill formal requirements and for use as evidence in court). Digital signature schemes are a common technique for the creation of electronic signatures. The goal of this paper is to investigate the suitability of a certain class of digital signature schemes, so-called identity-based signatures, for fulfilling legal requirements.

1.1 Identity-Based Signatures

The paradigm of Identity-Based Cryptography (IBC) was proposed by Shamir [31], and partially solves the problem of retrieving certificates or public keys that exists in Public-Key Infrastructures. It is based on the idea of using identities (represented by arbitrary data, such as e-mail addresses, full names or social security numbers) as public keys. This way, a signature can be verified with knowledge of some public, system-wide parameters and the signer's identity.[1] Identity-based signature schemes can be more efficient and easier to use than classical schemes. They achieve the same security properties as traditional signature schemes, except for a major drawback: The corresponding private keys cannot simply be generated by their respective users themselves. Identities are public knowledge, so allowing self-generated private keys would imply that *anyone* could generate these keys.[2] Therefore, a central authority is introduced that generates private keys on behalf of the users. This authority is referred to as Private Key Generator (PKG). It must be trusted to provide these private keys only to authorized users; if compromised, it would enable attackers to decrypt documents independent of the identity used for their encryption, and sign on behalf of any user in the system.

The combination of a traditional signature and the signatory's certificate can be seen as an identity-based signature, as only the certification authority's public key (which is a public, system-wide parameter) is required for verification: The signatory's public key is contained in the certificate. This construction has the advantage that users can generate private keys themselves. It has been referred to as "folklore construction" [28, p. 208]. The existence of the scheme does not imply equivalence of identity-based and traditional signature schemes; the *concept* of identity-based signatures is still for the PKG to generate the private keys.

[1] Identity-Based Encryption (IBE), on the other hand, means that an identity, along with some system-wide parameters, is sufficient to encrypt a message, which can be decrypted with the private key associated to that identity. The private key need not have been generated when the message is encrypted. Note that, while the first practical identity-based encryption scheme was only published in 2001, an identity-based signature scheme was already suggested by Shamir in his 1984 paper.

[2] At least conceptually; there is a way around this problem for identity-based signature schemes, which we will discuss later on.

1.2 Outline

So far, identity-based cryptography has been discussed almost exclusively in the technical community; however, to better understand its applicability, the legal consequences must be considered as well. We deal with the legal classification of identity-based *signatures*, not identity-based cryptography in general.

We provide an introduction to the legal regulation of digital signatures in Section 2 and discuss whether identity-based signatures can fulfill these requirements in Section 3. Our analyis is based on the European Signature Directive, but also takes into account the German Signature Act (discussed in Section 4) as a specific transposition as well as the UNCITRAL Model Law on Electronic Signatures. As it turns out, identity-based signature schemes can, in principle, fulfill all requirements of electronic signatures that exist in European Law, though details of the German national transposition appear more problematic. While the legal aspects of identity-based signatures have not been discussed in literature, we present related work bridging law and technnology of signature schemes in Section 5. We conclude the article in Section 6.

2 Electronic signatures

The application of digital signature schemes promises a significant economic potential if handwritten signatures can be replaced and business processes be digitized. Legislators in many countries have therefore specified conditions under which digital signatures are accepted as evidence and for the fulfillment of formal requirements. Cryptographic definitions of signature schemes usually do not take into account how the identity of the holder of a key pair is originally established, or how cryptographic keys are protected from abuse. These gaps are filled by legal definitions, which describe how "digital signatures" can be used to realize different classes of "electronic signatures". They also clarify in which cases cryptographic schemes are required for electronic signatures.

2.1 United States

Different national legislations adopt different paradigms. In the United States, the *Electronic Signatures in Global and National Commerce Act (E-SIGN Act)* [34] is a federal law containing regulations about the legal effect of electronic signatures in interstate and foreign commerce. The E-SIGN Act defines an electronic signature as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record" (Section 106). Section 101 (subsection a) states that a contract relating to a "transaction in or affecting interstate or foreign commerce" may not be denied legal effect "solely because an electronic signature [...]" was used in its creation.

The E-SIGN Act's definition of electronic signatures is very general and does not require the use of any cryptographic scheme. The Act does not contain any variants of electronic signatures with additional requirements. Blythe [7] refers to the U.S. approach as a "minimalist", "extremely market-oriented and permissive" law and notes that this approach has been adopted in most common law jurisdictions.

2.2 European Union

The European Union, on the other hand, has chosen to regulate electronic signatures more strictly. The directive on electronic signatures was adopted in 1999 [16]. It distinguishes four classes of electronic signatures:

- Electronic signatures are defined in article 2 of the directive as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication". Electronic signatures that *only* meet this definition (and none of the following ones) are often referred to as "simple electronic signatures". Note that no security requirements are mentioned; it is sufficient for the signature to *serve as* a method of authentication, so a scan of a handwritten signature included in an electronic document is considered as an electronic signature[3]. In this respect, the definition of electronic signatures is similar to the one of the American E-SIGN Act.
- Article 2 of the directive also defines advanced electronic signatures; an electronic signature is an advanced signature if
  - "it is uniquely linked to the signatory;
  - it is capable of identifying the signatory;
  - it is created using means that the signatory can maintain under his sole control; and
  - it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable."

  Thus, advanced electronic signatures require both the use of a cryptographic signature scheme and organizational measures, including a mapping between the signature and an identity.
- Article 5 (Section 1) introduces the additional category of "advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device"; signatures of this category are sometimes referred to as "qualified signatures" (for brevity, we adopt this term). The term "certificate" (defined in article 2 of the directive) is used in the same sense as introduced in Section 1. The directive lists requirements for qualified certificates (i.e., the required content) in Annex I, for their issuers in Annex II and for secure signature-creation devices (typically realized as smartcards) in Annex III.
- Article 3 of the directive allows member states to introduce voluntary accreditation schemes for certification service providers. Qualified signatures for which a certificate has been issued by an accredited certification service can therefore be considered as a fourth category, though details of the accreditation and its legal consequences are left to the individual member states.

[3] This assessment is non-controversial, see e.g. [24, p. 69] and [12, p. 4].

2.3 Transposition in German Law

As a member state of the European Union, Germany has transposed the European Signature Directive in national law. The Signature Act (Signaturgesetz), passed in 2001 to supersede the previous Signature Act and to comply with the European Directive, defines core concepts and regulates the business of certification service providers. It uses a translated version of the directive's definition of advanced electronic signatures.[4] It defines qualified signatures in a similar way to the above-mentioned category of the directive, but explicitly states that the qualified certificate must have been valid at the time of signing (this requirement, while not explicitly mentioned in the directive, appears self-evident and does not play a role in our further discussion). Moreover, the German law makes use of the directive's provision that allows introducing a voluntary accreditation scheme.

The Signature Act authorizes the government to pass an ordinance to regulate details concerning the Signature Act's execution: The Signature Ordinance (Signaturverordnung) contains, for example, security requirements that certification service providers have to comply with. Finally, based on appendix 1, Section 1 no. 2 of the Signature Ordinance, the Federal Network Agency (Bundesnetzagentur) publishes a catalogue of algorithms considered suitable for qualified electronic signatures, based on assessments by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) and taking into account international standards.

The German Code of Civil Procedure (Zivilprozessordnung), Section 371a (subsection 1) governs the use of qualified electronic signatures as evidence. A qualified signature constitutes a *prima facie* evidence: If a declaration is signed with a qualified electronic signature, it has to be considered authentic unless facts justify serious doubts that the declaration was made by the signatory. The Civil Code (Section 126a) defines the so-called "electronic form" of a document, which requires usage of qualified electronic signatures and which can replace the "written form" in many cases. The classification of digital signature schemes concerning their ability for usage in qualified electronic signatures is therefore highly relevant—both the validity of declarations and the potential to prove their authenticity in court depend on this classification.

2.4 UNCITRAL Model Law

The UNCITRAL Model Law on Electronic Signatures can be seen as a suggestion for the regulation of electronic signatures, provided by the United Nations Commission on International Trade Law. Its definition of electronic signatures differs slightly from the one in the European Directive. A requirement for all electronic signatures (which is not present in the European Directive's definition of simple electronic signatures) is that they "may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message" (article 2 of the model law). Electronic signatures are considered as reliable (article 6) if

- "The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

[4] Note that the translation differs between the German Signature Act and the German version of the European Signature Directive, but the differences do not affect the legal interpretation.

- The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
- Any alteration to the electronic signature, made after the time of signing, is detectable; and
- Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable."

Effectively, this means that a "reliable" signature is equivalent to an "advanced electronic signature" as defined by the European Directive.

3 Legal classification of Identity-Based Signatures

In this section, we investigate whether identity-based signatures can be used as electronic signatures according to different regulations.

As the United States (and other common law jurisdictions) have adopted a minimalist approach in the E-SIGN Act, using identity-based schemes to generate electronic signatures is not problematic. The "intent to sign" (Section 106 of the E-SIGN Act) an electronic record is sufficient, and cryptography is not required. The same holds for simple electronic signatures according to the European Signature Directive.

We therefore focus on the directive's definitions of advanced and qualified signatures, an example of its transposition in national law, and the UNCITRAL Model Law. Voluntary accreditation schemes, mentioned in the directive, pose organizational requirements concerning certification service providers. Since they do not add any requirements to signature algorithms, we do not take them into consideration.

We start our investigation with a look at the requirements of advanced electronic signatures, as defined by the European Signature Directive, as well as the model law's comparable concept of "reliable" signatures.

3.1 Advanced electronic signatures

The European Signature Directive lists four requirements, as mentioned in Section 2.2, for advanced electronic signatures (in addition to the definition of simple electronic signatures). Two of these requirements can be trivially fulfilled by identity-based signature schemes[5]:

- They must be capable of identifying the signatory. As mentioned above, the UNCITRAL Model Law contains a similar requirement (relating to all electronic signatures): It is required that they "may be used to identify the signatory in relation to the data message". Just like traditional digital signatures, identity-based signatures do not provide the identification feature per se. Though an "identity" (i.e. arbitrary text) of the signatory must be known to verify the signature, this is not necessarily a useful identity. However, adding the signatory's full name and, if necessary, other identifying attributes to the signed data is trivial.

[5] Kutylowski et al. [23, p. 271] get to the same result concerning asymmetric schemes in general.

- An advanced electronic signature must also be "linked to the data to which it relates in such a manner that any subsequent change of the data is detectable". This is also a requirement for the definition of cryptographic signature schemes, including identity-based ones. The integrity requirement for reliable signatures contained in the UNCITRAL Model Law applies only in cases "where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates". It is also fulfilled by any cryptographic signature scheme.

The two remaining requirements warrant a more detailed discussion.

3.1.1 Unique link to the signatory

Advanced electronic signatures must also be "uniquely linked" to the signatory. Note that a unique link between the signatory and a cryptographic key is not sufficient. The *signature* must only be linked to the signatory and not to any other person (as illustrated by Struif [33], Figure 1). In other words, a signature should be valid for one signatory only.

The requirement is not typically taken into account in the definition of cryptographic signature schemes. As a consequence, even schemes proven to be secure can be susceptible to the creation of a link to a second entity: A second public key can be generated for which the signature is also valid. Blake-Wilson and Menezes [6] call this property the "duplicate-signature key selection property". The property was later investigated and formalized by Menezes and Nigel [27], who coined the term "key substitution attack". Signature schemes vulnerable to key substitution attacks are not suitable for generating advanced electronic signatures; this is discussed, for German law, in [9]. For practical scenarios (in which a traditional digital signature scheme is used), a potential countermeasure is to include the certificate as part of the message to be signed. Bohli et al. [8] have proven the EC-KCDSA scheme [25], which uses this principle, to be secure against key substitution attacks.

For identity-based signatures, Choon Cha et al. [11] suggest the property of security against "existential forgery on adaptively chosen message and ID attacks". Bellare et al. [4] apply this notion to a number of identity-based signature schemes that have been proposed in literature. An attacker is considered successful, and the respective scheme considered insecure under this security notion, if he can generate a valid tuple of message, identity, and signature. For that purpose, the attacker is allowed (among others) to retrieve the private keys for *any other* identity. A successful key substitution attack on an identity-based signature scheme implies that a signature is valid for more than one identity; an attacker could thus retrieve the private key of one identity and, via the key substitution attack, get a second identity for which the signature is valid. This violates the claim of of security against existential forgery on adaptively chosen message and ID attacks. We conclude that key-substitution attacks cannot be successful against schemes that resist existential forgery on adaptively chosen message and ID attacks. As this is a widely acknowledged design goal, key substitution attacks are even less of a problem for identity-based signature scheme than for traditional ones.

Other legal literature does not take the problem of key substitution attacks into account. Despite the explicit wording of the directive, most sources consider the "unique link" requirement to be relevant for certification service providers[6] only, which must make sure

[6] The use of certification service providers is not required for advanced electronic signatures, but of course,

that no key pair is assigned to more than one person, and must know the link between the (public) key and the respective person's identity [17]. In practice, the assignment of a key pair to several persons does not occur if the certification service provider is honest, and if some basic precautions are taken. A cryptographically secure random number generator should be used during key generation; if that is the case, the probability of accidentally generating the same key pair for two persons is negligible. Some instances of implementation flaws in random/pseudorandom number generators have been reported [15, 21]. So far, the impact on advanced electronic signatures has been very limited. Key pairs for qualified electronic signatures are usually generated on special hardware, such as smartcards. We are not aware of any significant flaws in the cryptographic random number generators used on such hardware.

Mason [26, pp. 119–120] states the unique link of a signature to a person was impossible to achieve, as the required private key cannot be memorized and must be stored in a computer or on a smart card. The consequence is that third parties cannot be excluded from signature generation with absolute certainty. Following this opinion, advanced electronic signatures would not be possible at all—a result that was obviously not intended by the legislator. As a consequence, the problem pointed out by Mason is not considered in most legal literature. Assuming that the unique link requirement can be fulfilled by traditional signature schemes, the only potential reason to get to a different assessment for identity-based schemes is the existence of the PKG, which might provide another person, aside from the original signatory, with the capability to sign messages valid for the same identity.

We discuss this issue in the next section, as it is more closely related to the issue of "sole control" over the user's cryptographic key material. With the exception of this issue, we conclude that the "unique link" requirement of the European Signature Directive can be fulfilled by identity-based signature schemes.

Note that the corresponding requirement of the UNCITRAL Model Law requires a unique link of the "signature *creation* data" to the signatory, while the European Directive refers to the signature. The difference is subtle, but it means that schemes susceptible to key substitution attacks are not excluded from the UNCITRAL definition of reliable electronic signatures. On the other hand, the requirement can be easily fulfilled by identity-based schemes, assuming the PKG does not assign the same private key to more than one signatory.

3.1.2 Sole control

As a final requirement, advanced electronic signatures must be "created using means that the signatory can maintain under his sole control". The "means" to create the signature are private cryptographic keys; the wider wording of the directive was chosen for the directive to account for possible technical innovations. As pointed out by Kutylowski et al. [23], there are schemes that allow multiple private keys to be used with the same public key; in that case, the signatory must be able to keep all of them under his control.

The "sole control" requirement directly relates to the security of signature creation, both concerning technical measures (like access control to cryptographic keys) and concerning cryptographic schemes.

With respect to *technical measures*, there must be a way for the signatory to prevent others from using the "means" required for signing. There is, however, a broad consensus

they can be used.

that "sole control" does not imply a requirement to use special hardware, such as smartcards, to generate signatures [17]. If this were the case, it would not make sense to introduce the use of such "secure signature-creation devices" as an additional requirement for qualified signatures. Mason [26, p. 123f] points out the problematic nature of the "sole control" concept. Real-world IT systems are too complex to technically guarantee that security measures are not circumvented. Recitals 14 and 15 of the Signature Directive help in the interpretation of the clause, stating that "it is important to strike a balance between consumer and business needs" (recital 14) and that even the technical requirements for secure signature creation devices do "not cover the entire system environment" (recital 15). They indicate that absolute security is not required. The extent of the technical security level that *is* required is difficult to define; however, purely software-based solutions (like PGP) are generally considered acceptable[7]. In addition, the directive only requires the *ability* to keep private cryptographic keys under one's sole control; still, any signatory can decide to give up this control and to allow others to sign on his behalf (see also Kutylowski et al. [23, p. 272]). As long as secure cryptographic schemes are used, a signatory has the theoretic ability to exclude others from signing. Therefore, the focus on abilities instead of actual behaviour makes it easier to fulfill the requirements of advanced signatures. One might argue that if a signatory gave up the sole control over his private key, there would no longer be a "unique link" from the signature to the signatory; this argument is flawed, since the unique link to the original signatory still exists. Though he did not sign the document, the signature still allows identifying him.

At first glance, *cryptographic schemes* have to make sure that no one except the legitimate signatory can generate a valid signature. If this is true, identity-based signature schemes cannot be used for the generation of advanced electronic signatures: They use the PKG as a central authority which generates the private keys for all involved parties; obviously, this implies that the PKG can also generate signatures on behalf of anyone. Consequently, Anderson [2, Section 1.3] states that identity-based schemes "are not signature schemes in terms of the usual legal definition of an electronic signature".

The result becomes much less clear when looking at the "folklore construction" of identity-based signatures, as mentioned in Section 1.1. In this construction, an identity-based signature consists of a traditional signature and the signatory's certificate. Sending the signatory's certificate along with a signed document is common practice, so it seems that most advanced electronic signatures are, in fact, identity-based. Of course, this does not imply that *all* identity-based signature schemes are suitable for the generation of advanced electronic signatures. To find the delineation, we analyze the commonalities and differences between the identity-based paradigm and traditional signatures concerning the signatory's sole control over signature generation.

As already mentioned, the PKG of an identity-based scheme can generate signatures on behalf of any user of the system. However, the same is true for certification service providers of traditional schemes: They can generate a new key pair and a corresponding certificate containing any identity they choose. Prevention of such action is based on legal (not technical) measures, laid down in the general liability rules of civil law and specific regulation for certification service providers. The latter, such as Article 6 and Annex II

[7] As stated, for example, in the official justification [14] of the German Signature Act, which is based on the directive.

of the European Signature Directive, only apply to providers issuing qualified certificates. One might argue that the attack could be uncovered more easily in a traditional signature scheme, as certificates are usually stored in a directory, and additional certificates for a given identity would be noticed; this is not the case if the PKG of an identity-based scheme uses a signatory's private key. Since the purpose of the directory in a traditional scheme is to check the status of individual certificates, checking the whole directory for anomalies is not normally supported. As a consequence, the use of certificate directories does not help to detect fraud in traditional digital signature schemes, and does not constitute an advantage in comparison to identity-based schemes.

The main *conceptual* difference between traditional and Identity-Based Signature schemes is that in the latter, the central authority has the task to generate private keys for the users, while in traditional schemes, its task is only to provide certification. However, it is also possible for the certification service provider in a traditional scheme to generate key pairs on behalf of its users. This possibility is explicitly mentioned, even for certification service provides issuing qualified certificates, in Article 6, Section 1, bullet point c of the European Signature Directive. To maintain the signatory's sole control over signature generation, certification service providers are not allowed to store these private keys; for those issuing qualified certificates, this requirement is made explicit in Annex II, bullet point j, of the directive.

We conclude that the European legislator considers it

- acceptable for certification service providers to have the technical ability of generating signatures on behalf of users (by generating and certifying new key pairs). This is not surprising, as preventing that form of abuse with technical means is not feasible.
- unacceptable for certification service providers to possess the private keys of their users. This must include any means to generate signatures that cannot be distinguished from those generated with the user's private key. *Generation* of private keys by certification service providers, on the other hand, is allowed if they do not retain a copy.

The challenge is to make sure that if the PKG generates signatures on behalf of its users, these signatures can be distinguished from those generated by the users themselves. This does not imply that the PKG cannot generate the private key for a user. It is sufficient for the PKG to delete that key immediately after making it available to the user, provided the PKG cannot generate this key (or another one leading to identical signatures) later on.

Cryptographers have come up with schemes which have similarities with identity-based signatures, but which fulfill this property. The core idea of *self-certified* public keys [18] is to remove the distinction between a public key and a certificate. The public key is computed by the central authority and the user in collaboration, and the authority does not have access to users' private keys. While a specific construction proposed by Girault has a flaw [30], the concept itself is still valid. Besides schemes developed for public-key authentication, there are also actual signature schemes based on self-certified public keys [36]. Signatures based on different private keys can be distinguished, and the central authority does not get access to the key itself. Traditional signature schemes also have this advantage; the benefit of self-certified signatures is a potentially improved efficiency, as validation of signatures can be performed in one step, and as the public keys require less storage space than the combination of a public key and a certificate.

So-called certificateless signature schemes [1] are similar to self-certified signatures. They use a central entity, similar to the PKG, to generate partial private keys. However, each user adds some secret information to generate a private key unknown to the central entity. In contrast to identity-based schemes, the user's public key cannot be derived if only his identity is known. As opposed to traditional signature schemes, no certificate is required; a user's identity and the central entity's public parameters are sufficient for the verification of his public key. A key difference between certificateless schemes and Girault's concept of self-certified public keys is that the former allow the public key to be generated by the user without contacting the central entity; the private key can be computed later on. This difference, while important for certificateless encryption, has little practical relevance for signature schemes. We can therefore consider certificateless signature schemes and self-certified schemes as equivalent for the purpose of this article. In particular, both classes of signature schemes fulfill the "sole control" requirement of the European Signature Directive, as the central authority has no access to the users' private keys.

As opposed to the two aforementioned classes of signature schemes, identity-based schemes do not need signatory-specific public keys for signature verification[8], and the central authority (PKG) generates the private keys on behalf of users. As discussed above, they can still fulfill the "sole control" requirement, just like traditional signatures. To achieve this, the PKG must delete its copy of the user's private key, and must not be able to generate the same private key afterwards (even assuming that it has access to signatures generated with the original private key). Signatures generated using any private key generated by the PKG later on must be distinguishable from signatures generated using the original private key. Goyal [19] introduces the notion of *Traceable Identity-Based Encryption*, in which there is a large number of potential decryption keys, and the PKG does not get to know which one was selected by the user. The author states that the "analogue for identity based signatures appears straightforward to achieve". If it is achieved, such a scheme would be suitable for the use as an advanced electronic signature scheme.

Yuen et al. [35] present a model for identity-based signatures which allows proving the PKG's misbehaviour in an interactive "blame" algorithm between a judge, the PKG and the signatory; they present a corresponding construction based on an underlying traditional signature scheme. The scheme requires a trusted third party in addition to the PKG. As an obvious advantage, the chance of getting caught in case of fraud constitutes an incentive for the PKG to behave honestly. On the other hand, the scheme has drawbacks in practical applications. Signatures have to be considered as valid as long as the "blame" algorithm is not executed (otherwise, the signatory could invalidate his own signature by refusing to take part in the algorithm, does removing the non-repudiation property). Loss of the signatory's private key can therefore get problematic.

From a legal perspective, the scheme by Yuen et al. is acceptable for the generation of advanced electronic signatures. The means to generate signatures can be kept under the signatory's sole control; execution of the "blame" algorithm can be seen as part of signature verification, so it is possible to distinguish between signatures generated by the signatory and signatures generated by the PKG under the same identity. There is no requirement that

[8] Only system-wide public parameters and an identity are required.

excludes the use of an interactive algorithm (even involving the signatory and the PKG) during signature verification—especially considering that non-repudiation is achieved by the scheme.

3.1.3 Intermediate Result

We conclude that identity-based signature Schemes can, in principle, fulfill the requirements of advanced electronic signatures according to the European Signature Directive. This assumes that, analogous to Goyal's traceable identity-based encryption, a traceable identity-based signature scheme can be defined: After generating a private key for a user (signatory), the PKG must not be able to generate signatures that cannot be distinguished from those generated with the original private key. In contrast to design goals usually considered by cryptographers (and also by Goyal), it is acceptable for the PKG to learn the user's private key—just like a certification service provider, the PKG can be trusted to delete that key after generation. The "folklore construction" of identity-based signatures fulfills the requirements of advanced electronic signatures for the same reason. Despite problems concerning its practical application, the identity-based signature scheme by Yuen et al. [35] can also be used for the generation of advanced electronic signatures.

The UNCITRAL Model Law is less restrictive than the European directive, so if an identity-based signature scheme qualifies as appropriate for advanced signatures under European law, it is also a reliable signature scheme (as defined by the Model Law).

3.2 Qualified electronic signatures

For qualified electronic signatures, two additional requirements are defined in the directive:

- They must be created using secure signature creation devices.
- They must be based on a qualified certificate.

While the first requirement can be fulfilled (as smartcards suitable for that purpose can, at least in principle, execute identity-based algorithms just like they can execute traditional signature algorithms), the latter requirement is problematic. The main advantage of identity-based signatures is that they do not need certificates in general (though specific instantiations do); instead, the signer's identity and the public, system wide parameters (in particular: the PKG's public key) suffice to verify a signature.

The European Signature Directive (article 2, item 9) defines a certificate as "an electronic attestation which links signature-verification data to a person and confirms the identity of that person". In identity-based schemes, at least part of the "signature-verification data" can be chosen arbitrarily and represent an identity. Whether the mentioned attestation exists is a matter of perspective. The PKG's task is to make sure that a private key for a certain identity is only given to someone whose identity is described by the corresponding signature verification data. Though the directive was written with a traditional PKI in mind, the legal definition of a certificate can be interpreted to cover identity-based schemes. The PKG's public key is insufficient for the purpose, as it does not establish the link to a person—not even in combination with the person's identity. However, the combination of the PKG's public key, the representation of an identity and a signature fulfills the definition

Concept	Definition	Identity-based version
Certificate	electronic attestation which links signature-verification data to a person and confirms the identity of that person	PKG public key, identity-based signature, identity
Signature of a certificate	data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication	PKG public key, identity- based signature

Table 1: Concepts for identity-based signatures

of a certificate. This result holds despite a major difference to normal certificates, as our identity-based version of a certificate is not generated beforehand and not only by the certification service provider. Unlike a traditional certificate, the "certificate" of identity-based schemes is specific to each signature; however, this is not problematic. In fact, certificates for one-time use have been discussed for traditional PKIs as well [13].

Annex I of the directive specifies additional requirements for qualified certificates, as defined in article 2, item 10. Most requirements relate to information which must be contained in certificates and which can be encoded, for example, in the identities (i.e. the identity which is used as input to the cryptographic scheme is composed of the user's identity and the information which must, for legal reasons, be included). In general, the inclusion of "signature-verification data" (item (e)) is straightforward, as all data required for signature verification are already contained in the construction above—note, however, this is not true for the scheme by Yuen et al. [35]. Its "blame" algorithm is part of the signature verification, and requires private inputs from several parties. As a consequence, not all "signature-verification" data can be included in a certificate, and the scheme is not suitable for generation of qualified signatures.

For other schemes, in which a certificate can be constructed, fulfilling requirement (h) seems problematic: The certificate must contain the advanced electronic signature of the certification service provider. Surprisingly, the PKG's public key, combined with the identity-based signature, can be considered as an electronic signature. They are logically associated with the data to be verified (i.e. the certificate), which consists of the PKG's public key, the identity-based signature and the identity. The first two elements of the certificate are identical to its own electronic signature (see Table 1), and an association of these elements with the identity must be available to verify the identity-based signature.

The combination of the PKG's public key and the identity-based signature also serves as a method of authentication for the certificate—serving as a method of authentication is a major design goal of identity-based signature schemes. Usually, the goal of such a scheme is to authenticate a message with respect to an identity, using the PKG's public key and the identity-based signature. However, verification of the identity with respect to a certain identity-based signature and PKG public key is also enabled.

Moreover, the combination of the public key with the identity-based signature is even an *advanced* electronic signature: It is uniquely linked to the PKG, as no other party can generate private keys which can in turn be used to generate correct signatures for an identity. Obviously, there is also some relation to the individual signatory, but the link to the PKG (in this role) is still unique. Given additional information encoded in the PKG's public key, or known to all system participants, the "signature" is also capable of identifying the PKG. As the identity-based signature is only valid for one particular identity, any changes to either the identity, the signature or the PKG's public key cannot go undetected. However, the final property required is more problematic: An advanced electronic signature must be generated using means that the signatory can keep under his sole control. At first glance, this requirement cannot be fulfilled: An arbitrary amount of identity-based signatures can be generated without involvement of the PKG. However, the aspect that needs to be secured is only the link between the identity and the certificate, as defined above.

Annex II of the directive contains requirements to be met by the certification service provider. Most of these relate to management and security management issues, including the need for a revocation infrastructure. None of these requirements are particularly problematic for identity-based signature schemes. At first glance, bullet point (b), which requires the certification service provider to operate "a prompt and secure directory and a secure and immediate revocation service" might appear problematic, but approaches for revocation in identity-based signature schemes exist (as discussed, for example, by Boneh and Franklin [10]). In addition, the directive does not specify what the directory service must contain (in particular, it does not have to contain the certificates; providing a directory of identities for which private keys have been generated, on the other hand, is easily possible).

Annex III deals with secure signature-creation devices. In practice, smartcards (containing a secure key storage and the ability to compute the signature on the card) are used. While current smartcards do not typically support identity-based cryptography, this is not a problem in principle. As a consequence, Annex III does not restrict the use of identity-based signatures. The same is true for the recommendations concerning signature verification in Annex IV.

3.2.1 Intermediate Result

Surprisingly, an identity-based signature scheme is suitable for the generation of qualified electronic signatures according to the European directive, assuming that it fulfills the requirements of an advanced electronic signature scheme. This result is based on an interpretation of the term "certificate" that differs from the common use of the term, but is within the wording of the Signature Directive. As an exception to our result, schemes which require private inputs as part of the signature verification process (like Yuen et al.'s scheme [35]) cannot be used to generate qualified electronic signatures.

The UNCITRAL Model Law does not contain a direct equivalent of qualified electronic signatures, but there are regulations to be met by signatories, relying parties and certification service providers if they generate, verify, or provide certification services for signatures that have legal effect. Article 9, concerning the "Conduct of the certification service provider", also includes requirements for the contents of certificates. The definition of certificates in the Model Law is similar to the one in the European directive, so we can use a combination of the PKG's public key, the representation of an identity and a signature (as discussed above). In contrast to the European directive, however, there is no requirement to use certificates: Article 8, paragraph 1, bullet point c) explicitly states requirements "where a certificate is used to support the electronic signature", implying that this use is optional.

4 Identity-Based Signatures in German Law

Given that Germany's Signature Act is based on the European Signature Directive, it uses very similar concepts. The definition of advanced electronic signatures contained in the German Signature Act (Section 2 no. 2) is a direct translation of the corresponding definition from the European Directive. As a consequence, our result concerning the assessment of identity-based signatures as advanced electronic signatures (Section 3.1) directly applies to German law.

The category of "advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device" is referred to as "qualified signatures" in the German Signature Act (Section 2 no. 3). The requirements for qualified certificates are mostly identical to the ones already discussed above, with respect to the European Directive. However, one detail leads to a mismatch between the properties required by law and the design of identity-based signature schemes: Section 5, subsection 1 of the Signature Act requires certification service providers to keep qualified certificates publicly verifiable and retrievable, with the latter requirement only applying if the respective signatory agrees. A qualified certificate for identity-based signature schemes, as constructed above, can easily be kept *verifiable*, but the certification service provider cannot guarantee it to be *retrievable*, as the signature itself is part of the certificate—keeping all signatures in a directory is theoretically possible, but not desirable for most practical applications. Retrievability of the certificate is only supposed to ensure verifiabiliy, and adding the certificate to the message—thereby achieving the equivalent of an identity-based signature scheme—is considered sufficient in literature [20, margin number 9]. Given that retrievability is only conditionally required, and considering the purpose of the regulation, it does not prevent the use of identity-based schemes.

The Signature Ordinance, on the other hand, contradicts this result in its section 4, which explicitly requires the certification service provider to keep a directory of the qualified certificates it has issued. A wide, teleologic interpretation of this regulation could be considered, but given the explicit wording, we consider such an interpretation as problematic. Section 4 refers to a "directory according to the requirements of Section 5, subsection 1, sentence 3 of the Signature Act", which might be considered to imply that the Signature Ordinance does not introduce additional requirements. However, it is the purpose of the Signature Ordinance to provide more detailed specifications, and narrowing down the choice of accepted technologies is within that purpose. The same argument applies in relation to the European Directive: At first glance, a national regulation that excludes certain technologies which are allowed by the directive may appear as a breach of European law. As member states have some maneuvering room when transposing a directive, the German Signature Ordinance can be considered acceptable.

Note that a wider interpretation of the Signature Ordinance is not excluded. Even with our narrower interpretation, identity-based schemes could be easily introduced in Germany, as the process for changing the Signature Ordinance is easier than for the Signature Act itself. Such a change would also have to be reflected in the catalogue of suitable algorithms, which is updated yearly, anyway.

5 Related Work

To the best of our knowledge, we are the first to discuss the legal classification of identity-based signatures. Most of the research on requirements for electronic signatures focuses on management, policy, and architectural aspects of electronic signatures. There are, however, some publications trying to bridge technical and legal aspects—similar to the paper at hand. Rossnagel [29] introduces two approaches for signature generation using mobile phones and discusses whether they meet the requirements of qualified signatures according to the European Signature Directive. Kutylowsky et al. [23] discuss how the signatory's "sole control" over the signature creation process, as required by the European Directive, can be improved by providing evidence for fraud. The sole control requirement is also relevant for the classification of electronic signatures autonomously created by electronic agents: Bergfelder et al. [5] show that these signatures can be qualified signatures according to German law. With the exception of Mason [26], the requirements for advanced electronic signatures (and the "sole control" requirement in particular) are interpreted very similarly in legal literature, and our discussion of these requirements follows the consensus.

Bohli and Sorge [9] discuss if vulnerability to key substitution attacks affects the suitability of digital signature schemes for the generation of advanced and qualified signatures according to German law. We explain the applicability of this result to identity-based signatures in Section 3.1.1. Höhne et al. [22] deal with the legal classification of sanitizable [3] and redactable [32] signatures, also based on German law.

While not dealing with legal aspects per se, Girault [18] suggests three levels of trust in central authorities of public-key cryptography schemes. Level 1 means that the central authority knows the users' private keys (or is able to compute them). In level 2 schemes, the central authority does not know the private keys, but can impersonate users e.g. by issuing false certificates. Level 3 schemes have to provide proof of the authority's misbehaviour if it generates "false guarantees". Girault classifies traditional certificate-based schemes as level 3 schemes, stating that the existence of two or more different certificates for the same user proved that the authority had cheated. In practical applications, it is not uncommon for one user to possess more than one certificate issued by the same authority. Under these circumstances, only an approximation to Girault's level 3 can be achieved by means of cryptography: A signature scheme can allow distinguishing between signatures based on different private keys (in an identity-based scheme, this must hold even if they are issued for the same identity). This approximation corresponds to the requirement we have identified for identity-based signatures to be used for qualified electronic signatures.

6 Conclusion

In this article, we have shown that—contrary to Anderson's assumption [2]—identity-based signature schemes can, in principle, be used as the basis for electronic signatures. This result even applies to qualified electronic signatures according to the European signature directive. However, while it is acceptable for the PKG to generate a private key on behalf of the user, it must delete its copy of the private key, and must not be able to reconstruct this key later on. If the PKG generates signatures using a legitimate signatory's identity, there must be means available to distinguish the PKG's signatures from the legitimate signatory's ones. For qualified signatures, the distinction must be possible by only using the messages, signatures, and public parameters, but no private inputs from the signatory or the PKG.

Qualified signatures are highly relevant to practical applications, as they are considered equivalent to handwritten signatures, and they are admissible as evidence in legal proceedings (Article 5, Section 1 of the directive). This applies to all member states of the European Union, though exceptions may apply in specific fields of law.

Our interpretation of the European Signature directive may appear excessively wide, but given the directive's stated goal of being technology-neutral, and given that our intepretation is within the directive's wording, we believe our approach to be reasonable. Still, while the directive has been transposed into national law in the member states, details of the national laws may prevent the adoption of identity-based schemes.

7 Acknowledgments

This work was performed within the Collaborative Research Center 901, funded by the Deutsche Forschungsgemeinschaft. The author would like to thank Peter Günther and Dominik Leibenger for valuable comments.

References

[1] S. S. Al-Riyami and K. G. Paterson. Certificateless public key cryptography. In C.-S. Laih, editor, *Advances in Cryptology – ASIACRYPT 2003, 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, November 30 - December 4, 2003. Proceedings*, volume 2894 of *Lecture Notes in Computer Science*, pages 452–473, Berlin/Heidelberg, 2003. Springer.

[2] R. Anderson. Two remarks on public key cryptology. Technical Report 549, University of Cambridge Computer Laboratory, 2002.

[3] G. Ateniese, D. H. Chou, B. Medeiros, and G. Tsudik. Sanitizable signatures. In S. d. C. di Vimercati, P. Syverson, and D. Gollmann, editors, *Computer Security – ESORICS 2005*, volume 3679 of *Lecture Notes in Computer Science*, pages 159–177, Berlin/Heidelberg, 2005. Springer.

[4] M. Bellare, C. Namprempre, and G. Neven. Security Proofs for Identity-Based Identification and Signature Schemes. *Journal of Cryptology*, 22(1):1–61, 2009.

[5] M. Bergfelder, T. Nitschke, and C. Sorge. Signaturen durch elektronische agenten. *Informatik-Spektrum*, 28(3):210–219, 2005. In German.

[6] S. Blake-Wilson and A. Menezes. Unknown key-share attacks on the station-to-station (sts) protocol. In *Public Key Cryptography, Second International Workshop on Practice and Theory in Public Key Cryptography, PKC '99, Kamakura, Japan, March 1-3, 1999, Proceedings*, volume 1560 of *Lecture Notes in Computer Science*, pages 154–170, Berlin/Heidelberg, 1999. Springer.

[7] S. E. Blythe. Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security. *Richmond Journal of Law and Technology*, 11, 2005.

[8] J.-M. Bohli, S. Röhrich, and R. Steinwandt. Key substitution attacks revisited: Taking into account malicious signers. *International Journal of Information Security*, 5(1):30–36, 2006.

[9] J.-M. Bohli and C. Sorge. Key-Substitution-Angriffe und das Signaturgesetz. *Datenschutz und Datensicherheit – DuD*, 32:388–392, 2008. In German.

[10] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In J. Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, Berlin/Heidelberg, 2001.

[11] J. Choon Cha and J. Hee Cheon. An identity-based signature from gap diffie-hellman groups. In Y. G. Desmedt, editor, *Public Key Cryptography – PKC 2003: 6th International Workshop on Practice and Theory in Public Key Cryptography*, volume 2567 of *Lecture Notes in Computer Science*, pages 18–30, Berlin/Heidelberg, 2002. Springer.

[12] Commission of the European Communities. Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures, 2006.

[13] F. Corella. Lightweight public key infrastructure employing disposable certificates, US Patent US 6,763,459 B1, 2001. Application published in 2001. Also published as European Patent EP1117207 B1.

[14] Deutscher Bundestag. Gesetzwentwurf der Bundesregierung: Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften. Document 14/4662, 2000. In German.

[15] L. Dorrendorf, Z. Gutterman, and B. Pinkas. Cryptanalysis of the random number generator of the windows operating system. *ACM Trans. Inf. Syst. Secur.*, 13(1):10:1–10:32, Nov. 2009.

[16] European Parliament. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures . Official Journal of the European Union L 013, 19/01/2000, 1999.

[17] Forum of European Supervisory Authorities for Electronic Signatures. Working paper on advanced electronic signatures, oct 2004.

[18] M. Girault. Self-certified public keys. In D. W. Davies, editor, *Advances in Cryptology – EUROCRYPT '91, Workshop on the Theory and Application of Cryptographic Techniques Brighton, UK, April 8-11, 1991, Proceedings*, volume 547 of *Lecture Notes in Computer Science*, pages 490–497, Berlin/Heidelberg, 1991. Springer.

[19] V. Goyal. Reducing Trust in the PKG in Identity Based Cryptosystems. In A. Menezes, editor, *Advances in Cryptology – CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 430–447, Berlin/Heidelberg, 2007. Springer.

[20] L. Gramlich. Comment on Section 5 of the Signaturgesetz. In G. Spindler and F. Schuster, editors, *Recht der elektronischen Medien*, München, 2011. C.H. Beck. In German.

[21] Z. Gutterman, B. Pinkas, and T. Reinman. Analysis of the linux random number generator. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, SP '06, pages 371–385, Washington, DC, USA, 2006. IEEE Computer Society.

[22] F. Höhne, H. C. Pöhls, and K. Samelin. Rechtsfolgen editierbarer signaturen. *Datenschutz und Datensicherheit – DuD*, 36(7):485–491, 2012. In German.

[23] M. Kutylowski, P. Blaskiewicz, L. Krzywiecki, P. Kubiak, W. Paluszynski, and M. Tabor. Technical and legal meaning of "sole control" – towards verifiability in signing systems. In W. Abramowicz, L. Maciaszek, and K. Wecel, editors, *Business Information Systems Workshops*, volume 97 of *Lecture Notes in Business Information Processing*, pages 270–281. Springer, Berlin/Heidelberg, 2011.

[24] C. M. Laborde. *Electronic Signatures in International Contracts*. European University Studies Series II: Law/Europäische Hochschulschriften Reihe 2: Rechtswissenschaft. Peter Lang, Frankfurt, 2010.

[25] C. H. Lim and P. J. Lee. The Korean certificate-based digital signature algorithm. *Computers & Electrical Engineering*, 25(4):249 – 265, 1999.

[26] S. Mason. *Electronic Signatures in Law*. Law Practitioner Series. Cambridge University Press, 2012.

[27] A. Menezes and N. Smart. Security of signature schemes in a multi-user setting. *Designs, Codes and Cryptography*, 33:261–274, 2004.

[28] K. G. Paterson and J. C. Schuldt. Efficient identity-based signatures secure in the standard model. In L. M. Batten and R. Safavi-Naini, editors, *Information Security and Privacy*, volume 4058 of *Lecture Notes in Computer Science*, pages 207–222. Springer, Berlin/Heidelberg, 2006.

[29] H. Rossnagel. Mobile Qualified Electronic Signatures and Certification on Demand. In S. Katsikas, S. Gritzalis, and J. Lopez, editors, *Public Key Infrastructure: First European PKI Workshop: Research and Applications, EuroPKI 2004, Samos Island, Greece, June 25-26, 2004. Proceedings*, volume 3093 of *Lecture Notes in Computer Science*, pages 274–286. Springer, Berlin/Heidelberg, 2004.

[30] S. Saeednia. A note on Girault's self-certified model. *Information Processing Letters*, 86(6):323–327, 2003.

[31] A. Shamir. Identity-based cryptosystems and signature schemes. In G. Blakley and D. Chaum, editors, *Advances in Cryptology: Proceedings of CRYPTO '84, A Workshop on the Theory and Application of Cryptographic Techniques. Held at the University of California, Santa Barbara, August 19 - 22, 1984*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53, Berlin/Heidelberg, 1985. Springer.

[32] R. Steinfeld, L. Bull, and Y. Zheng. Content extraction signatures. In K. Kim, editor, *Information Security and Cryptology – ICISC 2001*, volume 2288 of *Lecture Notes in Computer Science*, pages 285–304. Springer, Berlin/Heidelberg, 2002.

[33] B. Struif. Use of biometrics for user verification in electronic signature smartcards. In I. Attali and T. Jensen, editors, *Smart Card Programming and Security, International Conference on Research in Smart Cards, E-smart 2001, Cannes, France, September 19-21, 2001. Proceedings*, volume 2140 of *Lecture Notes in Computer Science*, pages 220–227, Berlin/Heidelberg, 2001. Springer.

[34] United States Congress. Electronic signatures in global and national commerce act. 106th Congress Public Law 229, enacted June 30, 2000, 2000.

[35] T. Yuen, W. Susilo, and Y. Mu. How to construct identity-based signatures without the key escrow problem. *International Journal of Information Security*, 9(4):297–311, 2010.

[36] Y. Zhou, Z. Cao, and R. Lu. An efficient digital signature using self-certified public keys. In *Proceedings of the 3rd international conference on Information security*, InfoSecu '04, pages 44–47, New York, NY, USA, 2004. ACM.