Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The legal classification of identity-based signatures

*Christoph Sorge**

University of Paderborn, Department of Computer Science, Germany

Keywords:
Digital signatures
Electronic signatures
Information law
Identity-based cryptography
Identity-based signatures

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. The first digital signature scheme, RSA, was proposed by Rivest et al. (1978).

For these schemes to become practical, a public key must be securely bound to the identity of its owner. Traditionally, Public Key Infrastructures (PKI) have been used for this purpose. The core element of a PKI is a so-called certification authority (CA)—also referred to as certification service providers (in the legal context). A CA certifies 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 signer whose public key has been certified 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.

* Department of Computer Science, University of Paderborn, Warburger Str. 100, 33098 Paderborn, Germany. Tel.: +49 5251 60 1760.
E-mail address: christoph.sorge@uni-paderborn.de.

0267-3649/$ – see front matter © 2014 Christoph Sorge. Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.clsr.2014.01.002

1.1. *Identity-based cryptography*

The paradigm of Identity-Based Cryptography (IBC) was proposed by Shamir (1985), 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. The principle can be applied both to encryption ("Identity-Based Encryption") and to digital signatures ("Identity-Based Signatures").

A major drawback of IBC is that the private keys corresponding to identities 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.[1] 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).

Identity-Based Encryption (IBE) means that an identity (like "John Doe"), 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. For example, once a Private Key Generator has been set up, anyone (who knows some public information about the PKG) can send an encrypted message to "John Doe". The PKG will generate a private key for "John Doe" if someone requests this private key and proves that he actually is John Doe. Using that private key, the encrypted messages can be decrypted.

If a traditional Public-Key Infrastructure was used, the process would have to be different: John Doe would generate a key pair consisting of a public and a private key, prove his identity to a certification authority (CA), and receive a certificate from the CA. The certificate confirms that the public key belongs to John Doe, and is signed with the CA's public key. To send an encrypted message, the sender would need to retrieve the certificate (for example by sending an e-mail to John Doe and asking him to send the certificate). The sender would then verify the CA's signature of the certificate, encrypt the message with the public key contained in the certificate, and John Doe could decrypt it with the corresponding private key.

To summarize, *encryption* using a traditional Public-Key Infrastructure requires the recipient to generate a key pair prior to the encryption, and requires the sender to retrieve (and verify) a certificate containing the recipient's public key. Identity-Based Encryption avoids these drawbacks, but makes it necessary to introduce a Private Key Generator that generates the private keys (instead of allowing users to generate the key pairs on their own).

Identity-Based Signature schemes[2] also use identities as public keys: A signature can be verified with knowledge of some public, system-wide parameters and the signer's identity. If John Doe wants to sign a document, he asks the Private Key Generator to generate a private key for the identity "John Doe". With this private key, he can sign the message and send it to a recipient. The recipient only needs John Doe's identity, and some public information about the PKG, to verify the signature.

In a traditional Public-Key Infrastructure, John Doe would generate a key pair consisting of a public and a private key, prove his identity to a certification authority (CA), and receive a certificate from the CA. John Doe would typically include that certificate (which is signed by the CA and confirms that the contained public key actually belongs to him) in his message. The recipient would verify the CA's signature of the certificate and then use the contained public key to verify the signature of the message itself.

Assuming a trustworthy PKG, Identity-based signature schemes achieve the same security properties as traditional signature schemes. They can only be generated with knowledge of the private key, and can be verified by anyone who has some public information. Changes made to the signed document can be detected. However, like in Identity-Based Encryption, the need for a PKG constitutes a drawback of Identity-Based Signatures: The PKG must be trusted to provide the private keys only to authorized users; if compromised, it would enable attackers to 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" (Paterson and Schuldt, 2006, 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.

Some other constructions of identity-based signatures are more efficient than the "folklore construction" or traditional signatures, as there is no need to retrieve or verify certificates. For some applications, which require small message sizes, this advantage may be crucial.

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 electronic signatures in Section 2 and discuss whether identity-based signatures can fulfill these requirements in Section 3. Our analysis 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

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

[2] 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.