Electronic Signatures for Legal Persons

Michael Sonntag[1]

Electronic signatures are an important part of E-Commerce. Contracts can be concluded mostly in any form, but to proof their existence and content before courts, evidence is needed. Electronic signatures can produce this. However, they are currently only seen as signatures of natural persons. In E-Commerce it is also necessary for legal persons to sign documents, which can be done either directly or through representation. Some approaches for this exist, which will be discussed, including their legal consequences. A method will be described to allow legal persons to digitally sign documents using representation with full legal effects, based on a combination of a certificate of the represented person, a certificate of the representing person and an attribute certificate containing the authorization. This allows fulfilling the requirements for multiple signatures for representation and creating chain authorizations.

1. Motivation

Since January 1 2000, the Austrian signature law ([2], [26]) is in effect, which closely follows the digital signature directive of the European Union ([33], [25]). This allows the use of electronic signatures (for an introduction to certificates and signing see [34], [15]), implemented as digital signatures based on certain certificates, for signing contracts with full legal effect. An electronic signature can be substituted for a manual one, done by hand, in most cases ([16]; the EU directive excludes certain legal transactions: e. g. last wills or public forms as notarizations [15], [23]). This is especially important for electronic commerce.

For concluding a contract, a signature is not needed (matching declarations of intention suffice in most cases), but if a dispute arises, evidence is needed. This is commonly a paper copy of the contract, but now an electronic document can be used in court with a predefined result. Therefore especially Business-to-Business E-Commerce can receive a boost through this.

[1] Institute for Information Processing and Microprocessor Technology (FIM), Johannes Kepler University, Altenbergerstr. 69, A-4040 Linz, Austria; E-Mail: sonntag@fim.uni-linz.ac.at

In everyday business it is usual that not a natural person concludes a contract, but a legal one (and a natural person acting on behalf of it). It is therefore important to look at the following issues:

1. Can legal persons use signatures (e. g. for automatic signing) or only natural persons with full legal recognition? Can they possess their own certificates?
2. Should the signature of a legal person be a single signature or always a combination with the signature of a natural person (representation)?
3. How is the authority of a natural person to sign for a legal person encoded: In the certificate of the natural person, the certificate of the legal person or an attribute certificate (see [6] chapter 3 and [37])?

These and other questions will be discussed in detail with their advantages and disadvantages and their basis in the legal framework (European Union, using the Austrian signature law as an example, which is the first signature law to implement the signature directive of the EU; Germany, both old and draft for new signature law; four exemplary state laws from the USA) and in the context of corporate practices.

2. Certificates for legal persons

It took a long time until law recognized legal persons. The main problem with them is that they cannot take action for themselves. There is always the need for a natural person to act for them, although the results of them are ascribed to the legal person. The same is true even when the company acts through machines: There is always a natural person, who installed and set up the machine. However, using computers, this connection between actions and persons is much more remote, as even decisions can be made automatically to a large degree and the individual result might be unknown and rather hard to reconstruct by hand. To give these results a legal binding quality it would be necessary to (electronically) sign them. Currently such approaches exist in some areas of the public sector (e. g. automated notifications of penalties are legally valid if created by electronic data processing even without a manual signature), but they are not available to companies. This could change with the introduction of electronic signatures (in the form of digital signatures), as these are put in the same category as manual signatures on paper. In this context two questions are important: Can legal persons have their own certificate and are automatic signatures ascribed to the person authorizing them or to the legal person itself (in this direction [11]; “corporate signatures”)?

2.1. EU signature directive

In the directive a signatory is defined as “a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents.“ ([33] Art. 2 Z 3). Whether this includes a legal person as a signatory or not is unclear, but the wording suggest that this is possible and no arguments contrary to this seem to be included either in the text or the considerations. In my opinion it is possible, that legal persons can act as a signatory and therefore create advanced signatures. The other issue, whether a legal person can obtain a qualified certificate, has the same problem, although it is more likely that legal persons are included as always only the generic term “person“ is used. It seems therefore reasonable that legal persons can possess their own certificate and produce binding signatures. Important to note is, that an advanced signature is not required to be based on a qualified certificate. In contrast to this the special legal consequences take place only, if the advanced signature is based on a qualified certificate. However, as it is only a directive, it cannot be directly applied and must be implemented through individual laws by each country member of the EU.

2.2. Austrian signature law

In the Austrian signature law a signatory is defined as “a natural person to whom the signature creation data and the corresponding signature verification data have been allocated and who creates an electronic signature either on his own or on a third party's behalf, or a certification service provider who uses certificates to provide certification services“. Here it is obvious, that legal persons cannot legally sign an electronic document. However, a (simple or) qualified certificate seems to be possible as it is never referenced that only natural persons can possess one.

Also, a single example of this is included, as certification service providers can have a certificate as a legal person (the root certificate). Moreover, it has to be a qualified certificate: A user certificate has to be signed by the certification services provider with a secure digital signature, which is only possible if it is based on a qualified certificate. The reason for this is, that the change of the employee of the provider actually responsible for signing the individual certificates would create large problems. The root certificate would have to be revoked and a new one created and published, leading to an inflation of root certificates. Users would also have to constantly update their list of root certificates. From this it could also be derived, that legal persons can actually sign with their own certificate (according to the directive but not to the law). It would be paradox, if the provider can sign user certificates (a very high level of usage for a certificate), but could not sign other data. This would be especially problematic with timestamps, as they are not

certificates according to the definition, but simple data (the current time and a digest of the user data), which is signed to perpetuate legal recognition (repeated signatures) or provide evidence to use e. g. before court. However, the Austrian law (in contrast to the directive) restricts the use of certificates of service providers to certification services (not only the certificate but also the keys have to be different: [3] § 12 Abs. 1). Without this clause, they could therefore be used for signing documents.

From this it can be concluded that the signature law does not fully implement the directive. Since this has no effect at least until 19. July 2001 (time for implementation of the directive), currently legal persons cannot create signatures, although they can acquire a qualified certificate.

2.3. German signature law (Current)

According to the current German signature law ([17] Art. 3: SigG § 2), a certificate is a confirmation of the assignment of a public key to a natural person. It is therefore neither possible for a legal person to acquire a certificate nor create a binding electronic signature ([5], [31]).

2.4. German signature law (Draft for EU-directive - compliant amendment)

The current draft for the amendment of the signature law ([18]) defines ordinary and qualified certificates as only available to natural persons. As a qualified signature has to be based on a qualified certificate, legal persons can only create simple signatures, which possess no special legal quality.

2.5. USA

In the USA currently no nation-wide law on signatures is in place, but most states have adopted independent laws ([19]; important, as more requirements for written contracts exist [32]). These generally adhere to four different approaches ([13]), which are discussed in short based on representative laws.

2.5.1. Prescriptive approach: Utah

Certificate authorities have to acquire a license from the state: The individuals shall fully trust them, as they are evaluated before starting their operation. If the certification authority violates any of the legal requirements, it is liable to all those (users of the certificate and third persons), who trusted their certificates ([21]). This approach uses a lot of definitions and is restricted to a public key infrastructure. There

are six legal presumptions for digital signatures ([35] 46-3-406), if the signature is verified through a valid certificate of a licensed certificate authority and there was no reason for suspicions by the recipient:

- ✍ The certificate was issued by the licensed certificate authority named in the certificate
- ✍ The statements in the certificate are correct
- ✍ The digital signature used is from the owner of the certificate
- ✍ The signatory had the will to sign the electronic document
- ✍ The recipient of the signature has no knowledge that the signatory had violated his obligations or is not the rightful owner of the private key
- ✍ The digital signature was created before it was time stamped by a disinterested third party

According to the definition of the Utah signature law, legal persons can use signatures, as "person" is defined as "human being or any organization capable of signing a document, either legally or as a matter of fact." ([35] 46-3-103, 21). Also there are special considerations if an agent of a legal person requests a certificate ([35] 46-3-304, 2): If the authority for signing is limited, adequate safeguards have to exist to prevent a digital signature exceeding the bounds of the person's authority.

2.5.2. Criteria-based approach: California

In this approach, electronic signatures are put in the same category as signatures by hand, if they fulfill certain criteria ([27]). There are no specific technical requirements for electronic signatures ([9] 16. 5. d: defined as an electronic identifier intended to have the same effect as a manual signature), but there are also no special legal consequences or presumptions tied to them. Necessary elements for electronic signatures to be acceptable instead of manual are:

- ✍ Unique association to a person
- ✍ Verifiability
- ✍ The person using it can hold it in its sole control
- ✍ Changes in the data invalidate the electronic signature
- ✍ It conforms to the regulations of the secretary of state

The last point is the difficult one in this approach, as these regulations opened the door to a movement to the first approach: In the regulation ([10]) a lot of definitions are made and special requirements are set. E. g. public entities (to whom the Californian law is restricted!) may only accept certificates from "Ap-

proved Certificate Authorities", which is similar to licensing. The advantage is, that not only public key cryptography is included, but also signature dynamics – this is not possible under the Utah law.

According to the regulations by the secretary of state, a person is defined as "a human being or any organization capable of signing a document, either legally or as a matter of fact" ([10] 22000 a 3). Legal persons can possess certificates and create electronic signatures with the same effect as manual ones.

2.5.3. Signature-enabling approach: Florida

Electronic signatures ([14] 282.72 4; "any letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing") have the same effect as manual ones without any special requirements ([27]). Because of this, there are also no presumptions connected with them. They can be used and may not be discriminated because of their nature.

As no definition is given and the law uses alternatively "party", "subscriber" and "person", it seems reasonable to assume that legal persons can possess certificates and use digital signatures.

2.5.4. Hybrid approach: Illinois

This approach includes elements of the three other: There are a number of definitions, it is technology-neutral (important for future developments; [4]) and electronic signatures are handled the same way as manual ones. The Illinois Electronic Commerce Security Act ([22]) differentiates between simple and secure electronic records (content verification; handled the same as writings on paper) and simple and secure signatures (signer authentication; with digital signatures as an example), which determines the presumptions applicable ([30]). Similar to the EU directive, certain documents cannot be signed electronically, as special circumstances of the signature are required or desirable (wills, trusts, living wills or healthcare powers of attorney), or a unique writing is necessary (e. g. bearer certificates).

A certificate is partly defined as "names or otherwise identifies its subscriber or a device or electronic agent under the control of the subscriber". In contrast to the other approaches, in this case not only natural and legal persons can acquire a certificate, but also items (e. g. mobile phones) and electronic agents (e. g. software agents with a personal identity). For the scope of the law a person is defined as "an individual, corporation, business trust, [….], government, […] or any other legal or commercial entity." Because of this, the Illinois law has the largest applicability, as practically everyone and everything can possess a certificate and sign writings.

3. Current implementation of signatures for legal persons in Europe

Currently, in Europe legal persons cannot produce electronic signatures by themselves. However, the need for an equivalent exists. To supplement this lack, signatures of natural persons are used, in whose certificate their authorization to sign for a certain legal person is encoded and the rules for representation are applied. In general, both restrictions (less permissions than with an ordinary certificate) and authorizations (more or special permissions) can be contained as additional attributes in a certificate. In connection with signing for legal persons, this is justified with the fact, that they cannot act for themselves and on paper also always a natural person has to sign, representing the company or other entity. On paper, it is really impossible for a legal person to produce anything like a signature (using machines does not really help in this case, as each signature has to be invoked by hand), so there was no alternative to this. But with digital signatures, this has changed: It is possible for legal persons to produce a unique signature and also do this automatically. Although it will be in the end always a natural person, who programmed and started a software program, which then made decisions and finally created a signature, there is a high degree of autonomy. A connection to a natural person is more remote than to the legal person itself (e. g. automatically obtaining a timestamp and returning it as an acknowledgement of receipt).

With respect to an inclusion in a base certificate (or the possibility of removing it to an attribute certificate), it is necessary to distinguish between authorizations and restrictions.

3.1. Authorizations

Including authorizations directly in the certificate of a natural person has some advantages:

? Signing is simple as only one item (the certificate) is needed: No attribute certificates have to be selected and embedded.

? Obtaining the certificate is rather easy as all authorizations can be gathered, given to the certificate authority and a single certificate is created.

? From the signature it is easy (and always possible) to distinguish, which natural person is responsible for it, even for persons without information about the internal organization of the legal person. This is important for ascertaining, whether the signature for the legal person is valid or not (but with a signature directly of the legal person this would not be necessary).

However, several problems arise from the integration of authorizations in a natural person's certificate:

? It cannot be distinguished from the signature if this is a private signature or a representation for a legal person. The signed document itself has to be inspected to ascertain this. This is in contrast to signatures on paper: Usually immediately above or below the actual signature the role of the signer can be found. Also physically different signatures are used, e. g. “ppa” (per procura) as an addition, but part of the signature.

? Some persons might possess the authority to sign for multiple other persons (especially companies). This would lead to very long certificates and problems differentiating on behalf of which of these a certain document was signed. As long as the document is not created with a standardized structure, automated checking is not possible. The alternative, to use separate certificates for each authority, leads to the problem of managing a large number of certificates and their private keys.

? If a single authority within a combined certificate changes, the whole certificate has to be revoked and a new one procured. This has special problems for the signatures of third (unrelated to the change) authorities: Nothing has changed concerning them, but a different certificate is used from now on. Also the number of certificates to manage increases.

? Managing certificates with included authorization requires a certification authority for every single change and results in new and different certificates with the problem of distributing them (and especially their private keys): Creating certificate requests, archiving/destroying old private keys, etc.

? It is difficult to identify all persons authorized to sign for a legal person: The information is distributed across a number of certificates. Also there is no possibility to represent the company as such: It will always be only an attachment to a number of personal certificates without a unique representation as an individual entity. It is also probable that across a larger number of certificates the name of the company might be slightly different through e. g. misspellings or other forms of presentation, leading to further complications.

3.2. Restrictions

In contrast to authorizations or neutral attributes, restrictions have to be integrated in the base-certificate. Otherwise it would be possible to circumvent these restrictions by simple removing the attribute certificate or omitting it when signing.

Because of this distinction a problem arises: Are there attributes, which are authorization and restriction at the same time? They would pose special difficulties, as they may not be removed from the certificate (re-

striction), but should be (authorization). An (theoretical) example for such a restriction could be a special guarantee of the certification authority: For this certificate a maximum transaction level of e. g. 5.000 Euro is set. This amount is guaranteed by the CA, even if it is not responsible (deficiency guarantee; authorization), but on the contrary, no claims above this sum may be made (restriction).

A way to encode restrictions in separate certificates would be to include a unique reference to them in the base certificate. Including only the type of restriction would also suffice: Wrong attribute certificates would not refer back correctly. Checking signatures with such certificates should fail, if a reference to a missing restriction is found or it does not point back correctly. An advantage of separating the restriction is that it could be revoked independently from the certificate (e. g. declaration of majority). This would complicate the environment, as the revocation entry would (in addition to the revoked certificate) have to include the replaced restriction (ID of new attribute certificate) or if it was removed completely.

4. Attribute certificates

An attribute certificate is a separate structure, referring to a base certificate and containing additional attributes like clearances or authorizations. It can be used to implement signatures by legal persons through encoding the authority of natural persons to sign for them in the attribute certificate instead of in the base certificate. A signature may contain any number of attribute certificates (or references to them) without repetition ([7] 6.1.5). Whether an attribute certificate can be used with different base certificates or not depends on the type: It may refer directly to a certain certificate (only one possible) or to a distinguished name. This name may be used in multiple certificates and so the attribute certificate could be used with all of them ([37]; forbidden in [6] 3.3). Attribute certificates can be issued and revoked independently from their base certificate and also by a different authority (“attribute authority”; [12] 5.3.4).

4.1. Content of attribute certificates

Attribute certificates contain the following data, but no public key and not necessarily the name or pseudonym of the person (according to the X.509 standard [37]; some restrictions exist in [6]):

1) Version: Version number of the attribute certificate (currently v1 or v2).
2) Holder: This is either a reference to the base certificate using the issuer and the serial number of the certificate (and a number uniquely identifying the issuer if needed; see 8) or the distinguished name of

the subject. In the latter case it must be identical to the name in the base certificate, else automatic verification is impossible. Care has to be taken as this might not be unique (two persons might possess the same name). In attribute certificates of version 2, an object digest may be placed here to directly authenticate a holder (e. g. a hash value for Java-Applets or ActiveX-Controls).

3) Issuer: To identify the certificate (or attribute) authority, which issued this attribute certificate.

4) Signature: The signature of the certificate authority.

5) Serial number: A number uniquely identifying the attribute certificate with respect to the certification authority. It is not clear whether this must be unique within the attribute certificates only or within all certificates, which would be more sensible.

6) Certificate validity period: The period during which the attribute certificate is valid. It is unrelated to the validity period of the base certificate (but see below 4.3.3).

7) Attributes: The actual attributes associated with the subject. Any number of attributes can be included in an attribute certificate. Custom attributes are also possible but caution is needed, as misinterpretations can occur, if custom attributes of other authorities are included (only standard attributes have defined and reserved unique object identifiers).

8) Issuer unique ID: This field could be used if the issuer is not uniquely identified by the field "Issuer", containing e. g. a serial number of all certificate authorities with the same name. It should not be necessary to use this field, as identical names of certification authorities result in numerous problems.

9) Extensions: The same as extensions for certificates, but currently none are defined.

4.2. Standard attributes

A number of standard attributes, which will be often needed, are defined in [6] (for base certificates additional attributes are defined, e. g. serial number of the chip card containing the certificate and private key). The most important in this context is "Procuration". As an example for a restriction "Monetary Limit" will also be looked at, while "Declaration of Majority", "Admission" and "Date of Certificate Generation" will not be discussed here.

4.2.1. Procuration

This attribute is used to represent the authorization to act for another person (or any number of them), specifically for legal persons. Optional the country and type of substitution can be included to specify the type and which law is to be used for interpreting it. The represented person can be either identified by a name (this can be any name and need not be a distinguished name, so automatic checking might not be possible) or by a reference to a certificate.

4.2.2. Monetary Limit

With this attribute a limit for the liability of the certification authority can be realized. In addition it can be used for other restrictions, e. g. parents limiting the value of each transaction with this certificate. It can be used for all types of certificates (certification authority certificates, certificates for time-stamping and user certificates). The limit is represented through amount, exponent and a currency (Limit: amount*$10^{Exponent}$ currency units).

4.3. Legal aspects of attribute certificates

Attribute certificates differ in one important point from general certificates: They do not contain the public key of a person. It is therefore necessary to identify what legal consequences arise from this. Especially important is, whether including e. g. an authorization in it and using it for a signature brings about the legal consequences (like presumptions) also for the authorization or if they only apply to the data in the base certificate.

4.3.1. EU directive

Attribute certificates are never mentioned in the directive. A certificate requires an assignment of a person to signature-verification data and confirming the identity of the person. An attribute certificate does not fulfill this, as the base certificate already creates the link between the person and the public key. Even when the base certificate is uniquely defined (using the issuer and the serial number instead of the name of the subject), only the link between the attributes and the public key is created, while the identity is only repeated. Qualified certificates build up on normal certificates, so attribute certificate can also never fulfill their requirements. Regardless, together with a base certificate identifying the person (need not be a qualified certificate) they may be used for signatures and even advanced electronic signatures.

Because of the last, they may not be denied legal effectiveness and must be admissible as evidence in legal proceedings. They can, however, not fulfill the requirement of a handwritten signature, which only the base certificate does. When signing for another person it has to be interpreted as an ordinary (personal) signature with evidence pointing to the fact that it was created for another person. If only an authorization for one person is contained in the attribute certificate, the represented person is also uniquely identified.

4.3.2. Austria

With respect to attribute certificates the Austrian signature law is the same as the EU directive. Attribute certificates are never mentioned and are not certificates in the meaning of the law as there is no link between an identity and a public key.

Signatures including attribute certificates have therefore legal effectiveness and are admissible for legal proceedings. Yet using them with a base certificate does not create the (full) equivalent of a manual signature. If the base certificate is a qualified one, it is treated as a personal signature with additional data concerning an authorization and normal rules for representation apply.

It is important to note that the Austrian law differs with respect to attributes in a qualified certificate from the directive. Other attributes can only be included if they are of legal significance ([2] § 5 Abs. 1 Z 4) although the directive only mentions “a specific attribute of the signatory […] if relevant, depending on the purpose for which the certificate is intended”. Not every relevant purpose has to be legally significant (e. g. just convenient or for private uses), so there is a difference, which could be filled by attribute certificates. As no requirement is set for electronic signatures, any data can be included in them.

4.3.3. Germany (Old and draft for new law)

In the old (and also in the draft for the new) signature law attribute certificates are explicitly included. In contrast to the definition according to X.509 (see above), a restriction has been included: The attribute certificate must have a reference to a unique base certificate. According to this, the use of the name in the field “Subject” of the attribute certificate is forbidden ([6] chapter 3.3); it has to be the issuer and the serial number of the base certificate. Because of this reference, its validity always ends with the end of the validity of the base certificate (either revocation or lapse of time). All types of attributes can be contained in attribute certificates, both authorizations and restrictions. If restrictions are included in an attribute certificate and not the base certificate, an additional attribute must be included in the base certificate ([6]

2.3.9.15.2; “liabilityLimitationFlag”). However, it is only marked as non-critical and does not specify the type of restriction (or restrictions), only that at least one exists.

In Germany only the general set-up of digital signatures are regulated (certificates, certification authorities, licensing of them, …), but not the consequences of digital signatures ([5]). A digital signature is therefore only then equivalent to a manual signature, if all functions of it are met (conclusion, warning, identification and genuineness) This is accepted for signatures according to the signature law ([28]). As attribute certificates are explicitly included, adding authorization through it has full legal consequences (representation for a legal person). No difference exists between authorizations in the base certificate and in a combination of a base and the matching attribute certificate.

4.3.4. USA

The legal aspects are discussed based on the same four examples for signature laws as above.

? Utah: Attribute certificates are no certificates, but they are explicitly provided for (“may, […], contain or incorporate by reference additional information as determined by the licensed certification authority”; [36] R154-10-301 3). Presumptions are tied to certificates, so they do not apply to the content of the attribute certificate. E. g. the presumption that the subscriber (=subject of the certificate) created the signature with the intention to authenticate the data applies to the person in the base certificate, but not to the legal person mentioned in the attribute certificate, for which he is authorized to sign.

? California: An attribute certificate is no certificate according to the regulations, as it does not contain a public key. However, a base certificate may contain references to one ([10] 22003 a 1 D). It is required that a certificate “conforms to widely-used industry standards, including, but not limited to ISO x.509 and PGP certificate standards”, which define attribute certificates ([37]). As digital signatures include attribute certificates (see definition above), they are recognized by law and have full effect, although no presumptions exist at all.

? Florida: An attribute certificate is no certificate, as it does not contain a public key. However, it can be contained in a digital signature and has then the same force and effect as a written signature. No presumptions are included for any type of signature or certificates, so there is no difference and they may be used without any discrimination. It is irrelevant whether the information is contained in the base certificate or an associated attribute certificate.

? Illinois: A certificate has to contain a public key, so an attribute certificate does not match this definition. As the definition is not closed, references to attribute certificate can be added to them. This is specifically provided for when digital signatures are found to fulfill the requirements for secure electronic signatures ("the digital signature […], was used within the scope of any other restrictions specified or incorporated by reference in the certificate, if any"; [22] 15-105 1). Presumptions are tied to secure electronic signatures, which may contain attribute certificates. Therefore any presumptions do apply to the content of attribute certificates and base certificates alike.

5. Digital signatures for legal person

In contrast to the USA, where legal persons can create digital signatures for themselves, this is not possible in Europe, where always representation needs to be used. Because of this, the authorization to act for another person must be included in a signature. This authorization can be either done by including it directly in the certificate of the authorized person or in an attribute certificate.

5.1. Combined signatures for legal persons

To allow separation of the two distinct entities, a combined signature can be used. The signature for legal persons is then modeled as three separate object: The legal person, the natural person and the connection between them (authorization). The former two are conventional certificates, the latter an attribute certificate. A signature for a legal person consist of a combination of a signature of the company itself, the signature of the person acting on behalf of the legal person and the attribute certificate. The attribute certificate provides the association of the former two, confirming the authorization of this particular natural person to sign for a certain legal person. The authority need not necessarily be stored in an attribute certificate but could also be included in either the certificate of the legal or the natural person. However, this would require a 1:1 association of natural and legal persons or get very complicated. Additionally, this would prohibit realizing some of the advantages mentioned below. Both base certificates can be incorporated by reference as they can always be found through the information in the signatures, but the attribute certificate must be explicitly contained or specially referenced as finding it through the two base certificates might be hard or impossible. (In [7] the attribute and base certificates themselves are only required to be included if restrictions are encoded in them or they are not publicly available, otherwise a reference is

sufficient.) As the two signatures are independent from the sequence, a parallel signature can be done ([12] 8.13; “independent signatures”).

5.2. Example of a signature for a legal person

A digitally signed document where a natural person represents a legal person would look like this:

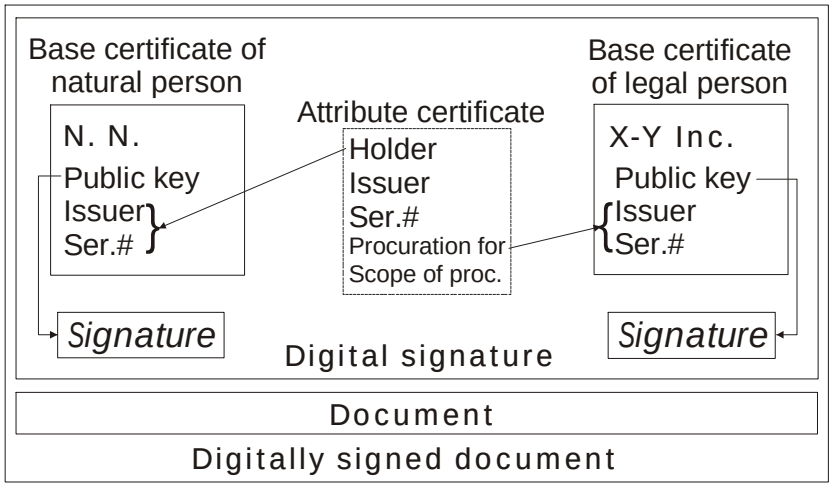

Figure 1: Signature for a legal person

5.2. Advantages

Some of the advantages of separating the authorization from the base certificate and from the certificate of the legal person are:

- ✍ Visibility: It is clearly visible if this is a private signature or a signature on behalf of a legal person: The latter needs signatures from both entities and an attribute certificate containing the authorization.
- ✍ Automatic verification of authorization: Checking the authorization of a certain person to sign for a specific legal person can be done automatically through the attribute certificate and the links connecting it with the two other certificates if the certificates are identified through issuer and serial number.
- ✍ Easier management of authorizations: Authorizations are easier to create, revoke and manage, as, in contrast to certificates, no private key is associated with attribute certificates. This avoids problems with secure creation, storage and disposal. Also, this can be done by another authority instead of the certificate authority issuing the certificates (see also next item).
- ✍ Self-issuing of attribute certificates: The requirements for attribute certificates are less than for full certificates, so a company might issue them by itself for their own employees. A directory service is not always needed, as the attribute certificate should be included in the signature. Revocations can

also be done, although here a directory service is required. However, if attribute certificates are issued for short times (e. g. only for days or a month), the need for revocations might be very small (for example only, when an authorized employee leaves in the middle of a month). With short-term authorizations the unique binding to certificates instead of to names (which might be not unique) is possible.

- Multiple authorizations separated: Each authorization can be easily embodied in a single attribute certificate. It is not necessary to possess either numerous certificates (with the same or different key-pairs) or a single certificate with many authorizations in it. Through this it is clear, on behalf of which person the signature was created (the single person from the attribute certificate), and if this is the case (if an attribute certificate is contained, it is always on behalf of somebody else).
- Legal person modeled as separate entity: Including the legal person as a separate certificate removes problems with misspelled or slightly different (e. g. some parts of a distinguished name are missing, like country or E-Mail address) names. Also attributes referring to the legal person itself can be used without having to include them in every attribute certificate (especially important as the certificates might be issued from different authorities, which are responsible for different attributes and therefore won't include those of other ones). This allows creating chains of representation: A person is authorized to act for a legal person, which in turn represents another legal person (*see Figure 2, right part*). This would be very hard and cumbersome to implement with attribute certificates only.
- Multiple-signature-requirements possible: E. g. in the case of joint power of representation including a signature by the company certificate provides additional safeguards and eases verification (see also 5.5). The certificate of the legal person connects the two or more attribute certificates and allows using unique references for identifying the person, which is acted for (name conflicts are impossible).

5.3. Problems

However, also some problems exist:

- Complicated management of certificates: For each signature the appropriate attribute certificate needs to be retrieved (from a probably long list) and two signatures have to be applied, requiring special software. If additional restrictions, statements or authorizations are needed, preparing a single signature is complicated because of the number of elements required (3 certificates and 2 private keys). Also the absolute number of certificates increases (while the number of private keys stays the same).

- ✍ Distribution of private keys: All authorized persons must be able to sign with it and therefore the private key must be available for multiple persons simultaneously. This can be a problem e. g. with chip-cards, where private keys are created on the card and can never leave it.
- ✍ Technical verification need not be equal to legal verification: If the certificates are incorporated by the name of the subject only, instead of the issuer and the serial number, they can be legally valid, although a technical verification might reject them ([12]). This happens if either the name is not absolutely identical or if the verification is restrictive and does not allow these references. However, including a reference to the certificate instead of the name reduces the possibilities for use: They can only be used in combination with a certain certificate and they expire with it, although they might be valid for themselves.
- ✍ Revocation list at attribute authority: Using attribute certificates requires an additional revocation list which has to be checked. As this might be separate form the certificate authority, additional difficulties can arise as a connection to another server might fail upon verification. See also under advantages: A company issuing attribute certificates needs to create its own revocation list, which can require an extensive infrastructure e. g. for securing the host.

5.4. Legal consequences

The signature created with the certificate of the legal person is not a full legally binding signature, especially as all authorized persons have to be able to sign with it and the private key can then no longer be under the sole control of a single person. Also the certificate used for the signature is not an advanced one as required by the EU directive and the Austrian signature law. Even when multiple persons are actually needed for signing (see below), the requirements are not fulfilled. Only in one case the signature could be a replacement for a hand-written signature: A single person is authorized to sign for the legal person and the certificate was issued for the natural person, mentioning the authorization directly in it (this case is not relevant here). In contrast to this, the signature(s) of the natural person are legally binding for the person(s) itself.

If they are accompanied by an attribute certificate including the authority to act for a certain legal person and the signature of this legal person, the recipient cannot deny knowing that the signature was done on behalf of someone else or for another person. In this context two problems are of interest: Is this combined signature a valid representation and does it fulfill a (perhaps necessary) requirement for a written signature?

The requirements for full representation in Austria are the following ([24] 161ff):

1) Full authorization by the principal: This is only an internal problem of the principal and the authorized person, if the recipient of the declaration of representation (= the attribute certificate) did not knew about a restriction. The attribute certificate is an outside representation ([1] § 1017) and its content has therefore to be interpreted objectively.

2) Disclosure of representation: The disclosure consist of two elements: Disclosure of the authorization and disclosure, that the authorization is used. The first is done automatically by using the attribute certificate and the latter by including it and the certificate of the legal person in the signature.

3) At least limited contractual capacity: This should be no problem in this context, as otherwise no certificate may be issued.

Therefore this combination of certificates fulfills the requirements for full representation for the recipient of a declaration in all cases, except if the recipient knew or should have known that the authorization does not exist or is of smaller scope. A contract is always concluded with the represented person. The principal has acted careless if the authorization does no longer exist: he should have revoked the attribute certificate, which is possible for both him and the authorized person ([1] § 1028, see also [24] 169: Appearance representation, a declaration of knowledge is in this case protected the same as a declaration of intention; [1] § 1026). If it did never exist or is of smaller scope (the attribute certificate can only be issued with his approval; [2] § 8 Abs. 3), the signature is also valid.

It also does fulfill the requirements for a hand-written signature. As representation is used (instead of directly signing by the legal person; not possible according to the EU directive; see 2.1), only a signature of the natural person is required. The signature of the natural person fulfills this and the additional signature of the legal person and the inclusion of the attribute certificate do not void it. The authorization itself need not be in written form, except in certain cases. If the authorization has to fulfill the same form as the basic transaction (if the form shall e. g. protect against rashness), there could be problems. High forms (notarization, etc.) are excluded even from digital signatures of natural persons, so they pose no problem. If a general written statement is needed, the attribute certificate fulfills this requirement, as itself is (legally) a written statement (it contains the secure electronic signature of the certification authority).

5.5. Multiple signatures

Using this scheme it is also possible to model the necessity for multiple signatures (joint authorization, e. g. when only two persons together are allowed to act for a company). If, for example, two authorized persons are required, the signature consists of the signatures and certificates of both natural persons, the signature and certificate of the legal person and two attribute certificates (*see Figure 2, left part*). In the attribute certificates (mixed joint power of representation or, when generally applicable and no different classes of authorizations exist, in the certificate of the legal person), the requirement for an additional signature is included, so automatic checking is possible (number of persons required and their type of authorization).

Using special methods for distributing the private key used for singing with the company certificate allows restricting the use to actual collaboration, as the whole private key can only be created from the (partial) data of at least several persons. The simplest (but rather insecure) version would be e. g. to omit one third of the bits of the key in the data for each of three persons: Only two persons together (but any combination of them) could recreate the whole key and create a signature.

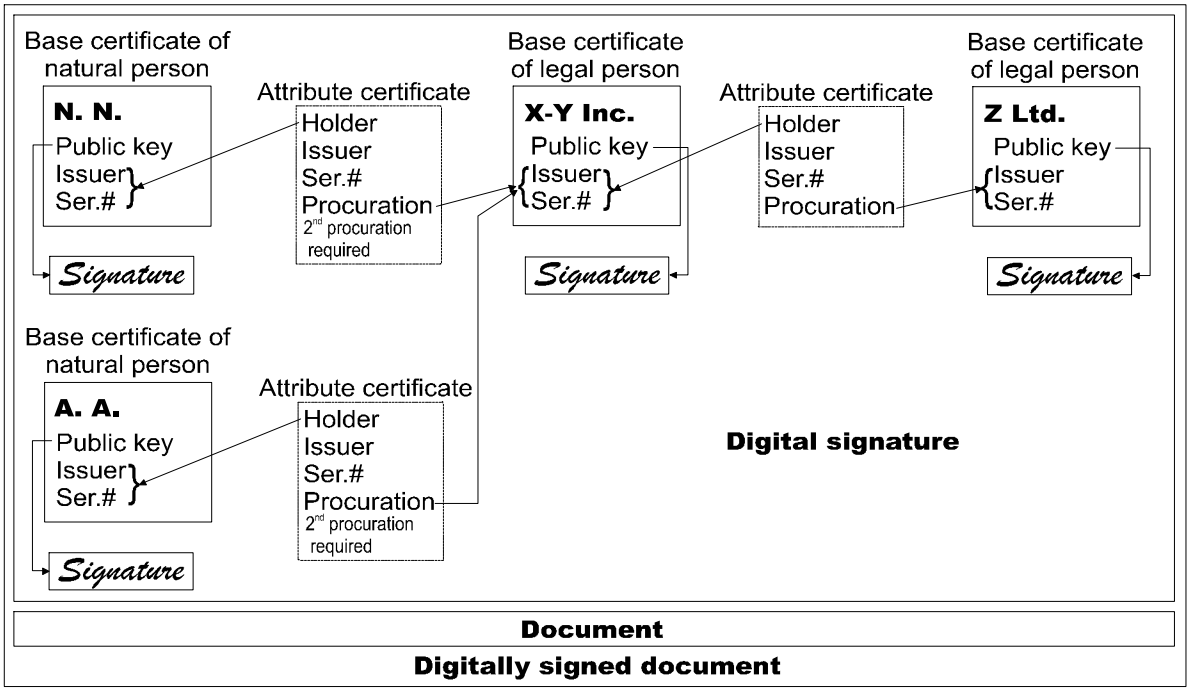

Figure 2: Multiple signatures and chain authorization

6. Conclusions

The current status of signatures for legal persons was described for a number of countries: Austria, Germany, some exemplary states of the USA and the European Union. In the USA, legal persons can create signatures on their own, while in Europe representation is needed.

It was described how the authorization to act for another person (be it a natural or a legal one) can be included in certificates, either in those of the person itself or in an attribute certificate. Because of their importance, the legal consequences of their use were also looked into.

Finally, a method for signing documents in representation of another person was described by the use of multiple certificates and attribute certificates containing the authorization to connect them. Using a separate certificate for the legal person (although legally invalid), reduces problems and increases versatility, as for example chain authorizations are much easier to create and the requirement for multiple signatures can also be modeled.

Signatures for legal persons can be created and are legally valid and binding, but they are not very easy to create and manage. Because of this, extensive support by software is needed before they will be used widely (and also to avoid security risks through incorrect handling or bypassing through users because of complicated handling [29]). Since the importance of E-Commerce is continually increasing, it is a necessity to also support electronic (and digital) signatures. Only then companies have the same instruments to e. g. conclude contracts in the electronic world as in conventional business.

7. Literature

[1] ABGB: Allgemeines bürgerliches Gesetzbuch vom 1. Juni 1811 JGS 946 idF BGBL I 164/1999

[2] Austrian Federal Electronic Signature Law: Bundesegesetz über elektronische Signaturen (Signaturgesetz- SigG), BGBl I 190/1999 http://www.a-sit.at/Englisch/Signature%20Law_E.pdf (25.5.2000)

[3] Austrian Signature Order SigV: Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung - SigV) vom 2.2.2000. BGBl II 30/2000 http://www.a-sit.at/Englisch/Signature%20Order_E.pdf (25.5.2000)

[4] BAKER, S., YEO, M.: Survey of International Electronic and Digital Signature Initiatives. In: Internet Law & Policy Forum. http://www.ilpf.org/digsig/survey.html (26.05.2000)

[5] BRISCH, K.: Gemeinsame Rahmenbedingungen für elektronische Signaturen. Richtlinienvorschlag der Europäischen Kommission., Computer und Recht 8/1998, 492

[6] BSI: Schnittstellenspezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV. Signatur-Interoperabilitätsspezifikation SigI. Abschnitt A1: Zertifikate. http://www.bsi.bund.de/aufgaben/projekte/pbdigsig/main/spezi.htm (22.3.2000)

[7] BSI: Schnittstellenspezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV. Signatur-Interoperabilitätsspezifikation SigI. Abschnitt A2: Signatur. http://www.bsi.bund.de/aufgaben/projekte/pbdigsig/main/spezi.htm (22.3.2000)

[8] BSI: Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV. Signatur-Interoperabilitätsspezifikation SigI. Abschnitt A6: Gültigkeitsmodell. http://www.bsi.bund.de/aufgaben/projekte/pbdigsig/main/spezi.htm (22.3.2000)

[9] California Digital Signature Act: http://www.gcwf.com/articles/cyber/digsig.html (25.5.2000)

[10] California Digital Signature Regulations (California Code of Regulations Title 2 Division 7 Chapter 10: Digital Signatures): http://www.ss.ca.gov/digsig/regulations.htm (25.5.2000)

[11] ERBER-FALLER, S.: Notarielle Funktionen im elektronischen Rechtsverkehr, DuD. Datenschutz und Datensicherheit 12/1994, 680

[12] European Telecommunication Standards Institute (ETSI): Electronic Signature Formats (ETSI ES 201 733 V1.1.3 (2000-05)) http://www.etsi.org/ (31.5.2000)

[13] FALLENBÖCK, M., SCHWAB, G.: Zu der Charakteristik und den Rechtswirkungen elektronischer Signaturen: Regelungsmodelle in den USA und Europa, Medien und Recht 6/1999, 370

[14] Florida Electronic Signature Act of 1996: http://www.leg.state.fl.us/citizen/documents/statutes/StatuteBrowser99/index.cfm?mode=Display_Statute&Search_String=&URL=Ch0282/PART03.HTM (30.5.2000)

[15] FORGÓ, N.: Was sind und wozu dienen digitale Signaturen?, ecolex 4/1999, 235

[16] FORGÓ, N.: Sicher ist Sicher? - Das Signaturgesetz, ecolex 9/1999, 607

[17] German Law on Digital Signatures (IuKDG Art. 3): http://www.iid.de/rahmen/iukdg.html#a3 (25.5.2000)

[18] German Signature Law (Draft 12.4.2000): http://www.dud.de/dud/files/siggaen2.zip (24.5.2000)

[19] GIDARI, A., MORGAN, J. P.: UPDATE: Survey of Electronic and Digital Signature Legislative Initiatives in the United States. Internet Law and Policy Forum. Digital Signature Working Group. http://www.ilpf.org/digsig/digsig.htm (25.5.2000)

[20] HAMMER, V.: Signaturprüfungen nach SigI, DuD. Datenschutz und Datensicherheit 2/2000, 96

[21] HEIN, W., RIEDER, M.: Digitale Signatur in den USA. Stand der Gesetzgebung und Praxis, DuD. Datenschutz und Datensicherheit 8/1997, 469

[22] Illinois Electronic Commerce Security Act: http://www.legis.state.il.us/ilcs/ch5/ch5act175articles/ch5act175artstoc.htm (25.5.2000)

[23] JUD, W., HÖGLER-PRACHER, R.: Die Gleichsetzung elektronischer Signaturen mit der eigenhändigen Unterschrift, ecolex 9/1999, 610

[24] KOZIOL, H., WELSER, R.: Grundriß des bürgerlichen Rechts. Band I Allgemeiner Teil und Schuldrecht. 10 Auflage. Wien: Manz 1995

[25] KRESBACH, G.: E-Commerce. Nationale und internationale Rechtsvorschriften zum Geschäftsverlehr über elektronische Medien. Wien: Linde 2000

[26] MENZEL, T., SCHWEIGHOFER, E.: Das österreichische Signaturgesetz. Umsetzung des EG-Richtlinienvorschlages in einem österreichischen Signaturgesetz. DuD 23, 9/1999, 503ff

[27] MIEDBRODT, A.: Regelungsansätze und -strukturen US-amerikanischer Signaturgesetzgebung, DuD. Datenschutz und Datensicherheit 7/1998, 389

[28] NÖCKER, G.: Urkunden und EDI-Dokumente, Computer und Recht 3/2000, 176

[29] PORDESCH, U.: Risiken elektronischer Signaturverfahren, DuD. Datenschutz und Datensicherheit 10/1993, 561

[30] ROBERTSON, R., SMEDINGHOFF, T.: Illinois Law Enters Cyberspace: The Electronic Commerce Security Act. In: Illinois Bar Journal. http://www.isba.org/member/june99lj/p308.htm (26.05.2000)

[31] ROßNAGEL, A.: Das Signaturgesetz. Eine kritische Würdigung des Gesetzesentwurfs der Bundesregierung, DuD. Datenschutz und Datensicherheit 2/1997, 75

[32] Schumacher, S.: Digitale Signaturen in Deutschland, Europa und den U.S.A. Ein Problem, zwei Kontinente, drei Lösungen?, Computer und Recht 12/1998, 758

[33] Signature directive of the EU: Richtlinie 1999/93/EG des Europäischen Parlaments und des Rats vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. 19.1.2000 L 13/12 http://www.a-sit.at/TEXTE/l_01320000119en00120020.pdf (25.5.2000)

[34] STERBENZ, A.: Digitale Signaturen - Eine Einführung. Institut für Angewandte Informationsverarbeitung und Kommunikationstechnik, TU Graz. http://akitsicherheit.iaik.tu-graz.ac.at/DiGSig-prinzip.htm

[35] Utah Digital Signature Act: http://www.jmls.edu/cyber/statutes/udsa.html (30.5.2000)

[36] Utah Digital Signature Act Rules: http://www.rules.state.ut.us/publicat/code/r154/r154-010.htm (30.5.2000)

[37] X.509: ITU-T X.509: Information Technology - Open Systems Interconnection – The Directory: Authentication framework, 1997 (Clause 13: Obtaining Certified Attributes)