BUNDESNOTARKAMMER
ZERTIFIZIERUNGSSTELLE

Electronic signatures

What you need to know before you start

Dear user,

With your decision to use the electronic signature of the German Federal Chamber of Notaries, which complies with the requirements of the eIDAS Regulation and the German Trust Services Act [Vertrauensdienstegesetz], you have made a decision for the future. To enable you to benefit from all the advantages of the electronic signature, you will find information about the electronic signature and your signature certificate in this brochure. The brochure also explains what you have to observe as the holder of a signature certificate. Therefore, please read this information carefully. Your signature certificate will be made available to you if you confirm in advance that you have taken note of this information by signing it or by clicking on it in the online application.

List of contents

1. What is an electronic signature? 4

2. Why are electronic signatures needed? 4

3. What legal effects does an electronic signature have? 5

4. What do I have to do to sign a document electronically? 5

5. What should be done if signed data is needed for a longer period of time? 6

6. What do I have to do to verify an electronic signature? 6

7. What does a (qualified) trust service provider do? 6

8. What happens in technical terms during electronic signing? 10

9. What do I have to consider when signing electronically? 13

10. What requirements must the technical components for electronic signing meet under the eIDAS Regulation? 14

11. What do I have to bear in mind when using the signature card? 15

12. What do I have to bear in mind when using the PIN? 16

13. What is the significance of including a pseudonym in the certificate? 16

14. What are the conditions for an electronic signature to be assigned to me in legal transactions? 17

15. How do I apply for a signature card from the German Federal Chamber of Notaries? 17

16. What is the legal background to electronic signatures? 18

17. Where can I get further information on technical or legal questions? 18

1. What is an electronic signature?

An electronic signature is data in electronic form which is attached to or logically associated with other electronic data and which the signatory uses to sign (Art. 3 No. 10 eIDAS Regulation).

The eIDAS Regulation distinguishes between two types of electronic signatures:
- the advanced electronic signature as well as
- the qualified electronic signature.

These differ in the legal requirements placed on them.

An advanced electronic signature is an electronic signature that fulfils the requirements of Art. 26 eIDAS Regulation (Art. 3 No. 11 eIDAS Regulation). It must therefore meet the following requirements:

a) It is uniquely associated with the signatory.
b) It enables the identification of the signatory.
c) It is created using electronic signature creation data which the signatory can use with a high degree of confidence under his sole control.
d) It is linked to the data so signed in such a way that subsequent alteration of the data can be detected.

A qualified electronic signature meets the same requirements as an advanced electronic signature. In addition, there are special requirements regarding the use of a (qualified) signature creation device to generate the qualified signature as well as the (qualified) certificate on which the signature is based (cf. Art. 28 et seqq. eIDAS Regulation in conjunction with Annex I or II eIDAS Regulation). A qualified electronic signature is thus subject to stricter legal requirements than an advanced electronic signature and must meet the highest technical and organisational security standards.

Accordingly, the law attaches different legal effects to an advanced and a qualified electronic signature. Only the qualified electronic signature fulfils special formal requirements in substantive law (Section 126a German Civil Code [Bürgerliches Gesetzbuch - BGB]) as well as in procedural law (including Section 130a German Code of Civil Procedure [Zivilprozessordnung - ZPO] and Section 3a Para. 2 German Administrative Procedure Act [Verwaltungsverfahrensgesetz - VwVfG]). Cf. on the legal effects of a qualified electronic signature **Question 3**.

2. Why are electronic signatures needed?

Digitalisation has become a core issue in our society. It no longer only affects traditional IT companies, but now encompasses many areas of business and private life. Technological developments are changing the way we inform ourselves, communicate and network. Ensuring trust and integrity is more important than ever. This is particularly evident in the electronic exchange of data via networks. Here, we cannot be sure that our communication partners are really always who they say they are. Nor is there any guarantee that the data will arrive as it was sent. However, a lack of trust in our communication partners and in their communication content makes legally binding electronic action more difficult. This applies in particular to the procedures of electronic legal transactions, in which it is an elementary prerequisite to ensure the identity and procedural legitimacy of the issuer of a declaration. The technology of the electronic signature can solve the central questions of the identity of the counterpart and the integrity of the contents. It enables the unambiguous determination of who the actual issuer of an electronic declaration is and whether the transmitted data has arrived intact or has been altered en route. With the evidentiary assignment of the signed data to a person, the electronic signature thus creates the prerequisite for legally binding electronic action.

3. What legal effects does an electronic signature have?

A qualified electronic signature has the same legal effect as a handwritten signature (Art. 25 Para. 2 eIDAS Regulation). Therefore, the written form can be replaced by the electronic form unless the law provides otherwise (Section 126 Para. 3 BGB). If the written form required by law is to be replaced by the electronic form, the issuer of the declaration must add his name to it and provide the electronic document with a qualified electronic signature (Section 126a Para. 1 BGB).

Furthermore, the qualified electronic signature allows special formal requirements in procedural law to be fulfilled (cf. e.g. Section 130a ZPO or Section 3a VwVfG).

With regard to the evidentiary effect of a qualified electronic signature, section 371a Para. 1 ZPO provides for civil law that the provisions on the evidentiary value of private deeds apply mutatis mutandis to private electronic documents bearing a qualified electronic signature. The prima facie evidence of the authenticity of a declaration in electronic form resulting from the verification of the qualified electronic signature pursuant to Art. 32 of the eIDAS Regulation can therefore only be shaken by facts that give rise to serious doubts that the declaration was made by the person responsible.

Qualified time stamps are subject to the presumption of the accuracy of the date and time indicated therein and of the integrity of the data associated with the date and time.

4. What do I have to do to sign a document electronically?

The specific procedure for signing a document depends on the software used. However, the basic steps in creating a signature are always the same.

In XNotar, documents can be signed electronically with the help of the signature folder. You can find more information on this at

https://onlinehilfe.bnotk.de/display/XNP/Signaturmappe.

5. What should be done if signed data is needed for a longer period of time?

The period of time for which electronically signed documents are to be stored can vary greatly. Long-term storage can result from long warranty or limitation periods, for example, or play a role if the document is to serve as evidence in the future. In the case of a desired or required long retention period, it must therefore be taken into account that the security of the algorithms on which an electronic signature is based and the associated parameters decrease over time due to new scientific findings or as a result of technical progress.

For this reason, the calculation routines and parameters for generating electronic signatures are only assessed as suitable for a certain period of time in advance, after which they are subjected to renewed testing and, if necessary, adapted to the changed technical circumstances. The Federal Network Agency therefore regularly publishes an overview of suitable mathematical procedures at https://www.bundesnetzagentur.de and specifies the date until which their suitability applies.

Qualified electronically signed, sealed or time-stamped data must therefore be re-signed in a qualified manner, if there is a need for this, before the security value of the existing signatures, seals or time stamps is reduced by the passage of time. The new security must be in accordance with the state of the art (cf. German Electronic Signatures Act [Vertrauensdienstegesetz - VDG]).

6. What do I have to do to verify an electronic signature?

To verify an electronic signature, the mathematical correctness of the signature, the certification path (certificate chain) taking into account the underlying validity model and the validity of the certificate at the time of signature must be verified. These verification steps are usually carried out by software components, so-called signature application components - for example XNotar.

In the XNotar programme, signature verification is possible via the integrated PDF viewer.
For more information, see the online help at
https://onlinehilfe.bnotk.de/display/XNP/PDF-Viewer.

7. What does a (qualified) trust service provider do?

Generation of the keys

The key pair used for electronic signing, consisting of private and public key, must be created (generated). It is very important in this context that each key pair may only exist once. Furthermore, no one - not even the trust service provider itself - may gain knowledge of the private key. The systems involved in key generation were thoroughly checked for these requirements and found to be fully suitable. In addition, there are regular checks of the prescribed security mechanisms. Another important security feature is the storage medium of the key pair. This storage medium - the qualified electronic signature creation device (QSCD) - ensures that the private key never leaves the storage medium. In the case of signature cards, the German Federal Chamber of Notaries uses smart cards that have been specially tested and certified for this purpose. In the case of remote signatures, the private key remains with the trust service provider on a remote QSCD, the hardware security module (HSM). After the key pair has been generated at the trust service provider, it is assigned to a registered user (personalisation) by linking the personal data of the user with the public key by an electronic signature of the Certification Body.

Certification of the public key

„Certification" literally means „attestation". Trust service providers certify that a public key belongs to the owner of the key pair. To be able to do this, the trust service provider must reliably establish the identity of the user. For this purpose, the German Federal Chamber of Notaries uses, among other things, notarial signature certification, in which the notary identifies the user. Once the trust service provider has established the identity of the user, it creates a chip card individually for the user as well as the key pair for electronic signing. The trust service provider certifies that the public key has been assigned to the user by means of the certificate (referred to in the eIDAS Regulation as the „qualified certificate for electronic signatures" and hereinafter also the certificate). A certificate contains data that enable the recipient of electronically signed data to identify the issuer of the declaration. This includes the surname and first name of the certificate holder in any case (Exception: the certificate holder has had a pseudonym included in the certificate instead of his name). Further data in the certificate includes in particular information on the trust service provider who issued the certificate, the identity code of the certificate, which must be unique for the qualified trust service provider, as well as information on the beginning and end of the validity period of the certificate.

Finally, the certificate contains the public key of the certificate holder, the designation of the algorithms and possibly information on certain restrictions or authorisations (see also the next section: Attributes). This makes it possible for anyone to verify the certificate holder's electronic signatures.

An overview of all the information contained in the certificates of the Certification Body of the German Federal Chamber of Notaries can be found in the Certification Concept for Qualified Certificates (CPS) available on the Certification Body's website at the following link: https://zertifizierungsstelle.bnotk.de/veroeffentlichungen.

In order for the recipient of a certificate to be certain that the certificate has not been altered and that all information is correct, every electronic certificate is electronically signed by the trust service provider issuing the certificate. This enables any recipient to establish beyond doubt that the certificate originates from the trust service provider and that it has not been tampered with or is incomplete.

A certificate is thus comparable to an electronic ID of the certificate holder. It contains information about the certificate holder, the certificate issuer and serves to assign a public key to a person. The authenticity of this certificate is certified by the trust service provider by means of an electronic signature.

Attributes

An attribute stands for a special characteristic or position of the certificate holder. Attributes are included in the certificate (cf. Section 12 Para. 1 VDG).

Attribute: Power of representation for a third person

If you are authorised to represent a (natural or legal) person, you can you can have this authorisation included in a certificate. The inclusion of information about the existence of power of representation for a third person in the certificate requires that the third person's consent is proven to the qualified trust service provider.

If you are authorised to represent a legal entity, the authority of the person giving consent on behalf of the legal entity must be proven (e.g. by providing an extract from the commercial register).

Attribute: Official, professional or other personal details

It is possible to include an official or professional title and other personal details in a certificate. Inclusion shall only be made if evidence to this effect is provided. Therefore, if an official or professional title or other personal details are to be included in a certificate, a confirmation from the respective responsible body must always be enclosed with the application documents. For the confirmation of the capacity as notary or notarial administrator, the chambers of notaries are responsible pursuant to Section 67 Para. 3 Sentence 5 German Federal Code for Notaries [Bundesnotarordnung – BNotO].

Attribute: Further personal details

It is also possible to include further personal details in the certificate, provided that the person concerned has consented.

In every case in which a third party consents to the inclusion of an attribute, the third party has the authority to have the certificate containing the corresponding attribute revoked, insofar as the underlying legal relationship (professional status, power of representation) has expired.

Inclusion of restrictions

In addition, any restrictions can be mapped in a certificate. You must ensure yourself that the restriction you specify is meaningful; the trust service provider does not check the content. An example is a monetary restriction. Here you can have entries made if you only want to make financial transactions up to a certain amount with your electronic signature. For technical reasons, only the first two digits of your entries will be taken into account, the following digits will be rounded up.

Please note that when using electronic signatures in electronic legal transactions, the significance of monetary certificate restrictions has not been conclusively clarified.

Provision of certificates (directory service)

In order to verify an electronic signature, it must be possible to find out at any time from a trustworthy authority whether the qualified certificate for electronic signatures exists, is valid and has not been revoked. This task is fulfilled by the certificate database of the German Federal Chamber of Notaries (also called the directory service) for the (qualified) certificates issued by the German Federal Chamber of Notaries. If the certificate holder has indicated when applying for his signature card that his certificate should not be retrievable, the directory service query will only provide information that a certificate exists for the person and whether it is valid or invalid (compare the next point).

Receipt and execution of revocations by the trust service provider (revocation service)

Certificates can already become invalid before the end of the validity period by revoking the certificate. Initially, the certificate holder can request revocation of the certificate himself at any time (Section 14 Para. 1 No. 1 VDG). If the certificate holder discovers that, for example, his signature card has been lost or stolen, he must have the certificate revoked to prevent misuse. The certificate can also be revoked by the trust service provider (cf. Section 14 Para. 1 VDG). In addition to the statutory grounds for revocation, further grounds for revocation are contractually agreed in the General Terms and Conditions or the relevant framework agreement. In particular, the trust service provider can also revoke a certificate if the certificate holder does not fulfil his contractual obligations. Furthermore, if a certificate contains an attribute that requires confirmation by a third party, this third party has the right to demand revocation of the certificate if the power of representation or the prerequisites for the office- and profession-related or other personal information have ceased to apply (cf. Section 14 Para. 2 VDG). Furthermore, under certain conditions the supervisory authority may order the revocation of a certificate (Section 14 Para. 3 VDG).

The revocation of a certificate is registered in the directory service and the revocation status is published promptly, at least within 24 hours, so that a query of the revoked certificate shows the current status of the certificate. This possibility of revocation exists at the German Federal Chamber of Notaries seven days a week and twenty-four hours a day.

A revocation request can be submitted by telephone on the telephone number free of charge:

0800 - 3550 400

or in writing at:

Zertifizierungsstelle der Bundesnotarkammer
Burgmauer 53
50667 Köln

Unfortunately, revocation requests received by email cannot be processed. Please check four days after the written request whether the revocation has been entered in the directory service. When requesting a revocation by telephone, you should, if possible, state your product number, which can be found in our notifications or printed on the chip card, as well as your revocation or blocking password.

.

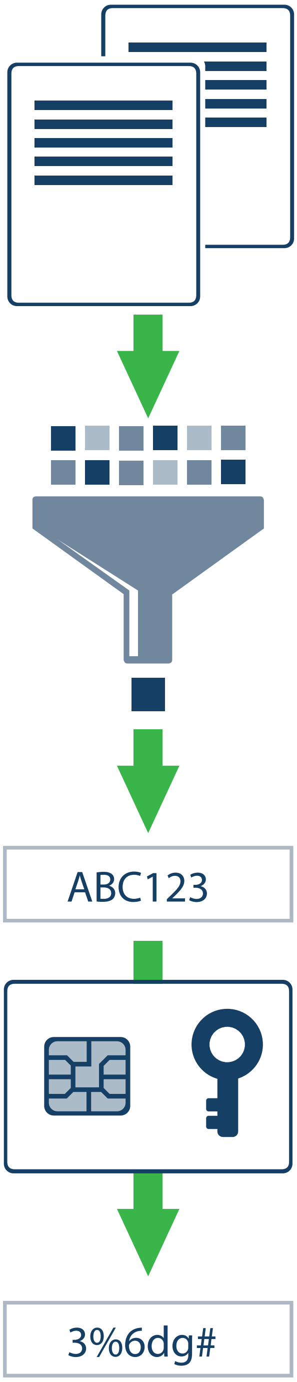
8. What happens in technical terms during electronic signing?

After the „Sign“ function has been selected, the signature programme calculates a short form of the file. This so-called „hash value“ is generated by a mathematical function and is comparable to a fingerprint: Each file has its individual hash value. Every change in the file, no matter how small (even if it is only an additional space between two words), leads to a modified hash value being calculated. The hash value is thus an individual short form of the file to be signed. This hash value is not a summary of the file's content, but a string of characters.

The individual hash value is then transferred for the actual electronic signing. In the process, the hash value is encrypted with the help of the private key of the qualified signature and passed back to the signature programme in this encrypted form. The private key is either applied directly to the signature card used or is used in the secure data centre with the remote signature stored there (for this purpose, the hash is sent to the data centre, encrypted there and sent back encrypted). The encrypted hash value of the file is the actual electronic signature. Since every change to the file leads to a change in the hash value, it is possible to determine whether the file has arrived unchanged at the recipient by comparing the encrypted hash value received by a recipient with a hash value that has been recreated for the file that was also transferred.

The certificate contains the public key. Therefore, together with your file, the recipient also receives the key with which he can decrypt the encrypted hash in order to then compare it with the hash of the received document that he has determined himself for the purpose of checking whether the document is unchanged. Because each key pair is only assigned once, the data can only be decrypted in this way and thus clearly assigned to an issuer (and owner of a private key).

The signature process



Text document (e.g. draft contract)

„Hash“ function: Shrinks large amounts of data down to a „fingerprint“. Each document is uniquely assigned a „fingerprint“.

„Fingerprint“ (= „hash“ value)

The „fingerprint“ is encrypted with the secret key of the signature card.

The encrypted fingerprint is the electronic signature.

The signature verification

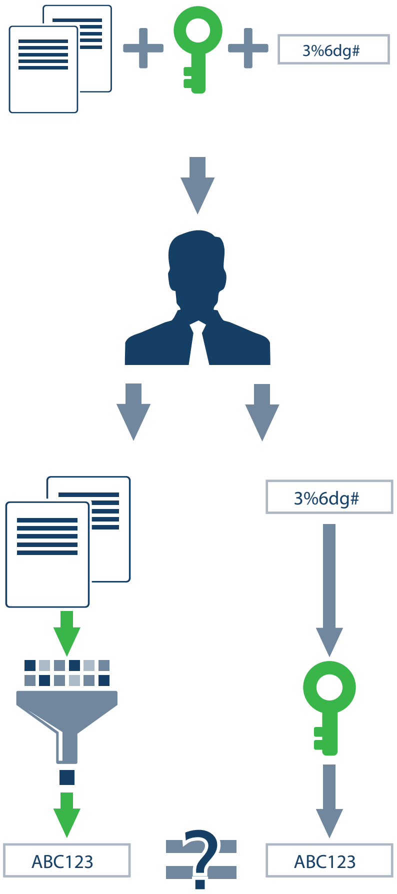
The recipient receives the document together with the sender’s electronic signature and public key. He must now check two questions:

1. Who did the document come from?
2. Is the content of the document unchanged?

He determines the „fingerprint“ of the transmitted document himself using the hash function.

With the public key, he decrypts the transmitted electronic signature.

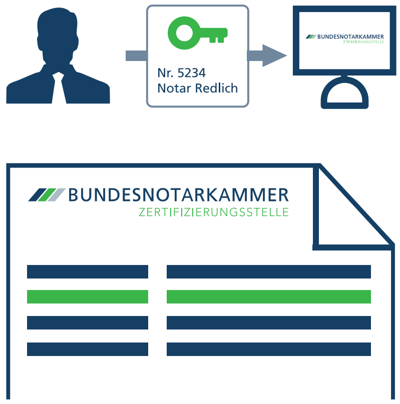
If both values match, the signed document has been transmitted unchanged.



The signature check: Certificate query

The recipient inquires online in the Certification Body’s directory service whether the sender of the message is stored there with the transmitted data (certificate number, public key).

The information is checked in the directory service. In addition, the validity of the certificate used is checked and the result is provided accordingly.



The Certification Body informs the requestor of the result of the certificate check.

!

Nr. 5234 - Notar Redlich
Gültig vom 01.04.2009
Gültig bis 30.03.2015
Zertifikat nicht gesperrt.

9. What do I have to consider when signing electronically?

The chip card and the qualified certificate are secure tools for electronic signing and encryption. However, certain rules must be observed when dealing with the electronic signature technology so that this security is not compromised.

Before signing electronically, check the content of the data to be signed electronically. To do this, use the display component of your software (e.g. XNotar), for example, which ensures that you really get the data displayed for verification to which the signature should refer. Uncertainties and problems of proof may therefore arise if signed attachments automatically change their content via macros or field functions. Files containing macros or field functions are not suitable for electronic signature (this may particularly affect word processing files such as Word documents). The XNotar programme enables the signing of PDF documents that comply with the PDF/A standard. In addition,it is also possible to sign multipage TIFF files whose contents can be represented unambiguously to a large extent and which do not contain any active elements. You always have the option of checking the electronic signatures you have created yourself to determine the correctness of the content of the electronically signed data. Efficient use of the electronic signature on a large scale requires the generation of several signatures with a single entry of the PIN (multiple signature). The signature and chip cards of the German Federal Chamber of Notaries therefore enable the generation of up to 100 signatures with one PIN entry.

With multiple signatures, however, particularly high security requirements must be met to ensure that only data that you actually want to sign is signed. Taking into account the existing conditions and the planned purpose of use, the operational environment must be physically and logically secured in such a way that misuse of the signature functionality of the card with multiple signature capability and spying out of the associated identification data (PIN) are practically ruled out and thus the sole control of the cardholder over the signature generation process is given. Physical security measures include physical protection against unauthorised access to the chip card. Since the qualified electronic signature is equivalent to your signature, declarations bearing your qualified electronic signature are attributed to you. The crucial protection against the erroneous or improper creation of signatures is your control over the signature process at all times and the protection of your smart card from being used by others.

10. What requirements must the technical components for electronic signing meet under the eIDAS Regulation?

The security of the electronic signature is ensured on the part of the Certification Body through strict testing of all technical devices, programmes used and even the employees.

However, secure creation of electronic signatures requires that the holder of a signature card also uses secure devices and programmes as a user to create signatures. The German Signature Act [Signaturgesetz], which was replaced by the German Trust Services Act [Vertrauensdienstegesetz], in conjunction with the German Signature Ordinance [Signaturverordnung], which was also repealed, laid down minimum requirements for the technical security of products used to create qualified electronic signatures. The manufacturers of the respective products had to explain in a so-called manufacturer's declaration how the respective requirements were implemented. In addition, the manufacturers had the option of having their products and compliance with the legal requirements tested by an independent confirmation body. Neither the eIDAS Regulation nor the German Trust Services Act contain a comparable regulation. Only for qualified electronic signature creation devices do minimum requirements result from the regulation in Annex II of the eIDAS Regulation. On the basis of the testing carried out by independent bodies, we therefore recommend that, as far as possible, confirmed components, i.e. confirmed smart card readers and confirmed user software, continue to be used for the use of qualified electronic signatures. The evaluation as secure, however, always refers only to the condition in which you received the product or the programme. Any change or intervention in the devices or the software will result in the security rating as a confirmed product or adequately tested product expiring.

In addition, products and programmes must be protected from unauthorised access and only used within a trusted environment. In particular, make sure that there are no viruses or other harmful programmes such as Trojans or worms on the computer with which you generate your electronic signatures. Before signing electronically, check the content of the data to be signed electronically. For this purpose, use the display component of the respective signature application, which ensures that you really get displayed for checking what you electronically sign in the following. You always have the option of checking the electronic signatures you have created yourself to determine the correctness of the content of the electronically signed data. Make sure that all devices and programmes you need for electronic signing are in proper working order. Prevent unauthorised access to these components by using appropriate security measures.

Ensure that devices and programmes for electronic signing and electronic signature verification are installed in a trustworthy and reliable manner and operate them only in accordance with their specification and documentation. Ensure that the computer you use at your workplace has been installed and administered in a trustworthy manner and that only trustworthy software is used.

Use security products such as virus scanners and firewalls to ensure the integrity of the systems you use for electronic signing. A reliable environment against dangers from the

Internet is guaranteed for notaries, in particular the connection to the notary network. Information on the notary network can be found at https://notarnet.de/.

11. What do I have to bear in mind when using the signature card?

The electronic signature is your personal electronic signature. When handling your chip card, you must therefore ensure that signatures can only be applied by you personally. Particularly high security requirements apply because you can use the signature card or chip card and remote signature of the German Federal Chamber of Notaries to generate several signatures with one PIN entry. Before it is used for the first time, each signature key of a signature card is protected with a five-digit transport PIN, which can only be used to change to an individual signature PIN with at least six digits. This change must be made by the cardholder without delay as soon as he has a signature card and transport PIN. It must be checked whether the signature card is protected with the five-digit transport PIN, as this is the only way to ensure that no signatures have yet been generated with the card. The signature PIN should be chosen differently from the PIN for encryption and authentication. With the combination of chip card and remote signature, the qualified electronic (remote) signature is triggered with the only PIN for encryption and authentication on the card. Since this is an effective PIN which can be used for signing immediately after receipt, the German Federal Chamber of Notaries recommends changing the PIN immediately after receipt of the PIN letter. You must keep the chip card theft-proof, exclusively in your personal possession and not hand it over to others.

For notaries, Section 33 BNotO expressly states that they may only administer the electronic signature creation data intended for the creation of official qualified signatures themselves. The notary may not hand over the qualified electronic signature creation device intended for this purpose to any other person and he may not disclose any knowledge data that he uses to identify himself to his qualified electronic signature creation device. He must protect the signature unit from misuse. Electronic notarial certifications according to Section 39a German Notarisation Act [Beurkundungsgesetz - BeurkG] are therefore invalid if the signature has not been made by the notary in person. If you ever lose your chip card, you must immediately arrange for it to be blocked and thus for the certificates on it to be revoked. For notaries, this already results from the regulation in Section 2 BNotO.

You can submit the revocation request to the German Federal Chamber of Notaries as follows:

By telephone on the number free of charge:
0800 - 3550 400

or by letter to the address
Zertifizierungsstelle der Bundesnotarkammer
(Certification body of the German Federal Chamber of Notaries)
Burgmauer 53
50667 Cologne.

Only use your signature card with devices that you are familiar with and have convinced yourself of their reliability. Observe the security instructions and use all devices and programmes only in accordance with their specifications and documentation. Regularly check the integrity of the products and the underlying platform (hardware and operating system) and protect your IT platform from malware. Ensure a trustworthy security administration of the system. If your signature card is damaged, there is a possibility that an attempt has been made to tamper with it. If you cannot assign the damage, take out a revocation of the signature key certificate for security.

12. What do I have to do electronically when using the PIN?

Electronic signing is only possible if the signing process is activated by entering the PIN. Anyone who is in possession of the PIN and the chip card can therefore sign electronically. You must therefore keep the PIN secret under all circumstances. If a third party has obtained knowledge of your PIN or if you suspect that this has happened, the PIN must be changed immediately. This is possible, for example, in XNP. If necessary, you should have the chip card blocked and the certificates on it revoked.

When choosing your PIN, make sure that it must not be possible for third parties to guess the PIN you have chosen. Numbers from your personal environment (dates of birth, telephone numbers and the like) should therefore not be used as PINs. Avoid using only one number as a PIN for different applications, chip cards or authentication processes. After entering an incorrect PIN three times, you can reset the error counter using the PUK you know and enter the PIN again. If you have used your PUK 10 times, it can no longer be used and you must order a new chip card.

13. What is the significance of including a pseudonym in the certificate?

If you choose to include a pseudonym in the certificate, ONLY the pseudonym and no other personal data will be included in the certificate. Signature cards with pseudonyms are therefore not suitable for making electronic authentications. Pseudonyms are identified by the entry „:PN“ in the certificate. Pseudonyms can only be assigned once within the circle of users of the German Federal Chamber of Notaries. If several participants apply for the same pseudonym, they are numbered consecutively, e.g. „Pseudonym :1 PN“, „Pseudonym :2 PN“, etc.

Pursuant to Section 8 Para. 2 VDG, the German Federal Chamber of Notaries may, under certain conditions and for certain purposes, transmit personal data of a person using trust services, including data on the identity of a user with a pseudonym, to the competent authorities upon request. The transmission shall be documented by the German Federal Chamber of Notaries. The authority requesting the transmission of the data shall inform the data subject of the transmission of the data. The information may be dispensed with as long as the performance of the statutory duties would be jeopardised and as long as the interest of the person concerned in the information does not prevail. Five years after the transfer, notification may be definitively dispensed with if the conditions for notification are unlikely to arise in the future, with a probability bordering on certainty.

14. What are the conditions for an electronic signature to be assigned to me in legal transactions?

This requires that the user of an electronic declaration adds his name and provides the electronic document with a qualified electronic signature, which can be generated by using the chip card of the German Federal Chamber of Notaries. Since you keep the PIN secret and have to enter it without fail for qualified electronic signing, according to the prevailing opinion as far as it appears, all qualified electronic signatures generated with your private signature key are basically assigned to you if the associated certificate was valid at the time the qualified electronic signature was generated.

15. How do I apply for a signature card from the German Federal Chamber of Notaries?

The starting point for the application is the online application at
https://zertifizierungsstelle.bnotk.de/produkte/alle-produkte.

Here you will find the different products and applications subdivided according to reference group. Once you have completed the relevant online application and printed out the application documents, go to a notary of your choice with the printed application and a current identification document. Sign the application in the presence of the notary. If you have already signed your application before, you can also acknowledge your signature on the application in the presence of the notary. The notary certifies your signature on the application. With your signature on the application, you consent to the production of a copy of your identity document presented. The notary will then send all documents to the Certification Body of the German Federal Chamber of Notaries on your behalf. If the application is to be accompanied by confirmation of professional status, hand over the confirmation form printed out with the application to the confirming body, which sends the confirmation directly to the Certification Body. The notary’s status is automatically confirmed by comparing it with the notary directory.

For members of the judiciary, the described procedure can also be carried out by the president or director of a German court. Lawyers have the option of being identified by the bar association responsible for them. If necessary, the Certification Body of the German Federal Chamber of Notaries provides other means of identification, which you can select during the application process.

If the identification procedure was carried out with the authentication of signatures for the first application of a natural person, it is usually unnecessary to have the signature authenticated again when applying for further qualified certificates. Subsequent certificate applications can therefore be made in private or by logging in with an existing chip card. Your application can only be processed by the German Federal Chamber of Notaries if it meets the requirements set out here. Your chip card or follow-up certificate will then be sent to you.

16. What is the legal background to electronic signatures?

The legal basis for electronic signatures is Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 199/93/EC (eIDAS Regulation) and the German Trust Services Act enacted for the purpose of effective enforcement of the eIDAS Regulation in Germany.

For the legal effects of an electronic signature, see **question 3**.

17. Where can I get more information on technical or legal issues?

Information specifically on the technical and legal background to electronic signatures can be found on the website of the Federal Office for Information Security (BSI) and the Federal Network Agency at:

https://www.bsi.bund.de/
https://www.bundesnetzagentur.de.

Publisher:

Zertifizierungsstelle der Bundesnotarkammer
(Certification body of the German Federal Chamber of Notaries)
Burgmauer 53
50667 Cologne.

Status: July 2022

https://zertifizierungsstelle.bnotk.de

https://zertifizierungsstelle.bnotk.de