Signature Guide for Experts

From ordering to archiving

The benefits of electronically signed expert reports at a glance

- Saves time and effort, especially for extensive expert reports in multiple copies
- Authenticity of the sender and integrity of the expert report are ensured
- The scope of appointment and the appointing body are shown in the signature, i.e. the details of the expert's official stamp are represented electronically
- Applicable to court and private expert reports: for use of the eBO (see below), the signature is no longer mandatory but continues to be recommended.
- Legally compliant and up to date

Step 1: Signature equipment

Applying for the signature card. Experts must apply for their signature card[1] in person and be identified. They need their identity card or passport, which must still be valid for at least four weeks at the time of application. The IHK signature card for experts can be applied for at many IHKs or via the PostIdent procedure at a price of €169 plus VAT.

In both cases, the IHK must confirm on a standard form that you are publicly appointed and sworn as an expert with a specific scope of appointment.

About three weeks after application you will receive, in separate letters:

- your personal signature card
- the associated PIN, including an acknowledgement-of-receipt form

Ordering accessories. To use the signature card, you need an external card reader with its own keypad. Card readers recommended by D-TRUST are available in the online shop. Install the corresponding driver software on your computer and connect the reader via USB. You also need signature software to sign your files (e.g. expert reports in PDF format). Please contact the respective providers. D-Trust works closely with secrypt, which offers digiSeal office:
https://www.chipkartenleser-shop.de/bdr_hw/zubehoer-d-trust-card-5x

[1] Technical requirements: internet access, Microsoft operating system Windows 7 or later, 2 GB RAM (4 GB recommended), USB port for connecting the card reader. The expert signature card is used with various technical components, some of which strictly require Windows. Apple users may be able to work with a Windows emulator; however, no guarantee is given for this.

Step 2: Activation and initialisation of the signature card

Please follow the D-Trust instructions at: https://www.d-trust.net/de/inbetriebnahme-karten

Step 3: Signing and sending expert reports

- Save the expert report as a PDF file.
- Sign the expert report: depending on the signature software used, either upload the file to your signature application, or right-click the file in your file manager and select the “Sign” option.
- Insert your signature card into the reader and click “Sign”. You will be prompted to enter your signature PIN; confirm with OK. The signed file is saved in the original location and can be recognised by its file extension.
- Send the signed expert report as an attachment – to the court via the electronic citizen and organisation mailbox (eBO); background and information on the required software: https://egvp.justiz.de/buerger_organisationen/index.php – and to other recipients (insurers, companies, private individuals) by email.

To validate the electronic signature, recipients do not need their own signature equipment, only free verification software. For evidential purposes, it may be advisable to create and save a validation report. Recommended product for free download: https://www.secrypt.de/produkte/digiseal-reader/ – the expert signature is explicitly displayed there.

Step 4: Archiving

A statutory retention period of 10 years applies to court expert reports. The signed expert reports must therefore be securely archived electronically for this period. Based on the requirements for audit-proof archiving of electronic accounting systems, immutability, long-term readability, confidentiality, security and completeness of the data must be ensured, ideally together with documentation of the procedure. For experts who have not yet implemented a suitable archiving solution, using a provider of audit-proof archiving may be advisable.