



## Terms of Use for DIDsign

### Application of These Terms of Use

For all services provided by the DIDsign Software under the website <https://didsign.io/> (the “Website”), these Terms of Use shall apply.

The Services are provided to you via software (the “Software”) created and run by B.T.E. BOTLabs Trusted Entity GmbH (hereinafter referred to as “BTE”, “us”, “we” or “our”) as defined below. The software is published and you are free to check out the code under <https://github.com/BTE-Trusted-Entity/didsign>

PLEASE READ THE TERMS OF USE CAREFULLY TO ENSURE THAT YOU UNDERSTAND EACH PROVISION. IF YOU DO NOT AGREE TO ALL OF THE TERMS, DO NOT ACCESS OR USE THE SOFTWARE.

YOU ACCEPT THE TERMS OF USE, EITHER BY CLICKING TO SIGNIFY ACCEPTANCE, OR BY TAKING ANY ONE OR MORE OF THE FOLLOWING ACTIONS: ACCESSING OR USING THE APPLICABLE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF USE.

YOU REPRESENT AND WARRANT THAT YOU ARE 18 YEARS OLD OR OLDER AND HAVE THE RIGHT AND AUTHORITY TO ENTER AND COMPLY WITH THE TERMS OF USE.

### What DIDsign is

DIDsign is a website that allows you to:

- sign electronic documents with your KILT on-chain DID directly in your browser,
- insert credentials as a part of the signature for these documents,
- use timestamping to proof the approximate time you signed them,
- verify documents that have been signed with a KILT on-chain DID,
- display additional information about the signers on-chain DID, such as e.g. the on-chain DID, service endpoints that are associated with this on-chain DID and KILT credentials that have been made available via the service endpoints.

This works for single documents, or multiple documents.

## How DIDsign Works

With DIDsign you can sign documents as follows:

- in order to use DIDsign you go to the Website,
- you allow the browser in which you use DIDsign to connect to your wallet with your KILT on-chain DID,
- you drop one or more files to your browser where you use DIDsign,
- DIDsign hashes the file(s),
- DIDsign hands over the hash to the wallet,
- you can now sign the hash in your wallet using your on-chain DID,
- your browser in which you use DIDsign receives the signature from the wallet and
- DIDsign makes files and signature available to you for download as zip or as individual files.

If you want to timestamp your signature:

- you upload the document to DIDsign and sign its hash with your DID as outlined above,
- you need to choose the paid option to timestamp the signature,
- for payment you need to connect to your payment wallet and select the right payment account from the list of accounts (filled by all the payment wallets),
- you click on a button for signing a blockchain transaction,
- the DID-signature of the hash is added to a “remark” and DIDsign creates a transaction to store it,
- you sign this transaction using the KILT payment account you previously selected,
- DIDsign stores this transaction on the blockchain and takes note of the block number and the transaction hash and stores them in the signature metadata file,
- you continue as outlined above and
- the download zip or signature file then contains the timestamping information

If you want to insert a KILT credential into your signature you proceed as follows:

- when you click to sign and your wallet pops up, if you have credentials, you can choose to insert one or more of your credentials into the signature,
- after that, the credentials you selected in the wallet are displayed as a nested part of the signature of the DIDsign and saved inside the signature file. If you want, you can rename them or delete them within DIDsign for the purpose of the signature and
- when you are done with including and naming your credentials, you can continue sign the hash in your wallet and proceed as outlined above.

You can forward the documents including the signature to one or multiple third persons and they as well can forward them. Forwarding is done outside DIDsign, e.g. by email or through other digital channels.

Any recipient can use DIDsign to verify whether the signature belongs to the documents and, if necessary, request further public information about the signature.

With DIDsign you verify signed documents as follows:

- you receive a signature and signed files independently from DIDsign, e.g. via email,
- you drop the received signature and signed files as individual files or zip into your browser where you use DIDsign,
- DIDsign in your browser checks if the signature comes from the signer's on-chain DID and if it is the signature specific for the uploaded files,
- if the signature was timestamped, the block number and the transaction hash are extracted from the metadata and used to query the block information via the KILT SDK API. The block contains the rough timestamp of its creation time, and DIDsign confirms that the document was signed no later than this time.
- DIDsign shows result of check, signature and the signer's on-chain DID and – if applicable – the timestamp,
- if the signer linked service endpoints to their on-chain DID, they will be displayed,
- you can request DIDsign to fetch credentials from those custom service endpoints,
- DIDsign tries to access those credentials, to verify them and to show the verification result and
- with the information received you can check, if the displayed data matches your requirements.

All documents dropped into your browser are stored locally in your browser and automatically deleted after the session. Personal data is not stored, siloed, or shared.

The data generated for you in DIDsign is stored locally on your device.

At launch, the Website supports only the Sporrán wallet also developed by BTE; other wallets may follow over time. For those other wallets, the process might differ slightly.

The usage of the DIDsign Website is free of charge.

## **Your Commitments**

You confirm that you are entitled for usage of the documents and signatures and your usage of these do not violate the rights of third parties, neither in the signing nor in the verifying process.

If you have signed a document with an on-chain DID that is no longer yours as you have actually lost, sold or otherwise relinquished it or suspect its fraudulent use, you will immediately terminate the use of this signature and all documents signed with it in order to avoid giving the wrong impression to the public or third parties. You will also inform anyone who was relying on your signature of the changes occurred or even warn them, in case you have ongoing relationships with them. We accept no liability in this respect.

As a verifier, you will determine for your purpose if and to what extent you will trust received data – depending on your legal, business or other requirements, you will determine, if the documents signed with a certain on-chain DID represent enough trust that these are coming from the right person/entity or if you need further documents of proof and which ones for example in regards to their identity. As these processes are defined outside of the algorithm, we accept no liability in this respect.

## **Liability**

BTE is liable for damages that are based on an intentional or grossly negligent breach of duty by BTE, its legal representatives or various agents.

In the event of a breach of essential contractual duties, BTE shall only be liable for the contractually typical, foreseeable damage if this was simply caused by negligence. Significant contractual obligations are those whose fulfilment enables the proper execution of the contract in the first place and whose compliance you can regularly rely on.

The limitation of the two preceding paragraphs also apply to the legal representatives and various agents of BTE, if claims are asserted directly against them. The liability limitations resulting from the two preceding paragraphs do not apply insofar as BTE fraudulently concealed the defect or assumed a guarantee for the quality of DIDsign.

Liability for culpable injury to life, limb and health and liability under Product Liability Act remain unaffected.

Any additional claims for damages are excluded.

## **Risk information**

The following risk information contains a list of risks associated with the use of DIDsign. The list is not exhaustive. It is not excluded that further unknown or unpredictable risks exist.

Independent of the creation of signed documents via DIDsign but also to prevent others from using secret or personal documents, please always keep the password and other access data to your devices, cloud solution and other data storage safe. Also, just like with any other document, only send your signed documents to someone you trust that they respect your privacy and to someone who will not forward your personal data to anyone else or lose or publish it in any way detrimental to your privacy.

DIDsign is used via the Website and its services are accessed via your wallet – please check all the information, instruction and warnings given about your wallet by its provider and closely follow the advice given. Always ensure that you do not lose your access data to your wallet and keep access to your wallet as well as the values and credentials stored in it safe from access by others.

The on-chain DID used for signing communicates with the KILT blockchain and depends on its functionality in regard to the proof of validity of your credentials.

Errors, dysfunctionalities, including failure of the KILT blockchain or the technical ecosystem in which it lives may adversely affect the DIDsign functionalities.

Also, service endpoints used to provide additional information in the DIDsign process are outside of this website and its functionalities. Errors, dysfunctionalities, including failure of the KILT blockchain, websites or the technical ecosystem in which they live may adversely affect the DIDsign functionalities.

DIDsign verifies the cryptographically correct usage of a DID and fetches credentials connected to it via service endpoints. The verification of DIDsign in regard to a credential therefore only refers to the cryptographic validity of credentials and their current status on the blockchain. DIDsign does not check the content of such credential, the trustworthiness of its attester or any other information around it that might be relevant. Therefore, DIDsign does not verify the content of such credentials or the correctness of their content in any way. To ensure that such credentials are indeed trustworthy for the purpose of your verification, as a verifier you should always do your own research and for yourself check, if the criteria for the respective purpose of use are met. If you find one or more credentials or other pieces of information included in the DIDsign verification process to be not trustworthy, should not trust the verification of the respective DIDsign process as such.

For timestamping you acknowledge that the timestamp is based on block time of the KILT blockchain, therefore depending on the regularity of the block times at the time of your signature, you will get an approximate time slot in which the signature was done. For signature and for the verification process, you need to determine if such timestamp is sufficient for your purposes.

You acknowledge and agree that we have no support, service level, or other obligations like these hereunder. Furthermore, you acknowledge and agree that changes in the Software and/or other information to the Website and usage of the DIDsign will from time to time occur and that verification for documents signed under previous version might at some point of time not be supported anymore.

DIDsign and in particular the underlying software application may be the subject of hacking or other malicious interference by unauthorized third parties resulting in the loss, theft or other violation of data or change in the Software.

Because the software of DIDsign is published, there is a risk that a third party may copy it and unconsciously or knowingly incorporate errors leading to potential adverse consequences for the usability and functionality of the DIDsign. To ensure you are using the original, always use through us directly and if uncertain, compare the code with the code published on GitHub before usage and only use if it matches fully with the code there.

Communication via internet-based systems is fundamentally susceptible to data/information being read out and possibly even changed. We have no influence on which processes (now and in the future) run in the background of the web browser or the wallet used.

## **Right to Change the DIDsign Software and These Terms of Use**

BTE reserves the right to change the DIDsign Software on the Website as well as the commercial and non-commercial conditions for its usage.

BTE also reserves the right to change these Terms of Use at any time for any future products of DIDsign in our sole discretion.

Such changes will be made via uploading new Terms of Use, the Software and/or other information to the Website and any usage of the DIDsign will from that time on fall under these new Terms of Use, will be handled by the new version of the Software and will be for the commercial and non-commercial, while existing Credentials acquired previous to this change shall remain untouched.

Documents signed under previous versions might not be supported and we accept no liability in this regard.

## **License to the Website and the Software**

**Copyright (c) 2022, B.T.E. BOTLabs Trusted Entity GmbH. All rights reserved.**

## **Miscellaneous**

These Terms of Use and the entire legal relationship between the parties shall be governed by the laws of the Federal Republic of Germany to the exclusion of the UN Convention on Contracts for the International Sale of Goods (CISG) unless the choice of law is legally prohibited.

If a term of this agreement to be invalid or unenforceable, the remaining provisions will continue in full force and effect.

The place of performance and exclusive place of jurisdiction for all disputes arising from these Terms of Use and the entire legal relationship between the parties shall be BTE's registered office, unless choice of jurisdiction is legally prohibited.



B.T.E. BOTLabs Trusted Entity GmbH  
Keithstraße 2-4  
10787 Berlin, Germany

German Commercial Court: Amtsgericht Charlottenburg in Berlin  
Registration Number: HRB 231219B  
VAT No: DE 346528612  
Managing Director: Ingo Rübe

Contact: [info@botlabs.org](mailto:info@botlabs.org)  
Or go to <https://support.kilt.io/support/home> and click on "Contact Us"

*Requirements according to § 5 TMG (Germany)*