Product Description
d.velop sign

1 Introduction

d.velop sign enables the user a complete end-to-end digitalisation of business processes without media discontinuity by digitally mapping the signature process. The functional scope of d.velop sign is described in more detail below. The d.velop cloud platform service description' is also applicable.

2 Scope of functions

2.1 Sign level

d.velop sign offers the possibility to sign documents digitally. The user can trigger an electronic signature - without a signature card and card reader - via remote signature. The following eIDAS signature levels are possible with d.velop sign:

- Simple electronic signature (SES): With either an electronic seal or a personal certificate
- Advanced electronic signature (AES): With either an electronic seal or a personal certificate
- Qualified electronic signature (QES): personal certificate

Signatures with a personal certificate are made using the "sign-me" service from D-TRUST GmbH, Kommandantenstrasse 15, 10969 Berlin, Germany; signatures with an electronic seal are made using the service from Swisscom Trust Services AG, Hardturmstrasse 3, 8005 Zurich, Switzerland (seal certificate). Both providers are trust service providers. Both services meet the requirements of the eIDAS Regulation.

To use the "sign-me" service, the customer, its business partners and their customers (hereinafter also referred to as the "user") must perform a one-time registration with D-TRUST GmbH. Registration establishes a customer relationship between D-TRUST and the user

The user must also identify themselves in front of an external body commissioned by D-TRUST GmbH before using d.velop sign for the first time. The user can choose from the identification procedures offered in the identification area. As of the time this contract was concluded, these are as follows:

- VideoIdent: The user's identification document is checked in a video conference.
- AusweisIDent: A card reader or smartphone is used to verify the user's identification card online.

d.velop reserves the right to change the identification procedures it offers to users, to offer additional identification procedures, or to discontinue existing identification procedures at any time. We are not required to maintain or introduce a particular identification procedure.

Two-factor authentication is required to generate a qualified electronic signature. Currently, an SMS-TAN or in-app authentication is used as the second factor. sign-me provides its own interface, which must be used to enter the second factor.

2.2 Technical requirements

As this is an SaaS solution, the user only needs an Internet-enabled endpoint.

2.3 Logon

The user can log in with single sign-on.

2.4 User interface

The appearance of the user interface can be customised (light or dark design; own logo).

The standard languages are German and English.

2.5 File types supported

The user can sign PDF/A documents with a size of up to 100 MB. The sum of all individual files within a folder is max. 500 MB.

2.6 Functions in the d.velop sign applikation

The following functions are available when using d.velop sign:

- Several documents can be summarised in one folder in a signature process.
- Accompanying documents that cannot be signed can be inserted as attachments in a folder.
- Signature processes can be initiated with internal and external participants.
- The order of participants in the signature process can be defined.
- The signature fields for the respective participants can be prepared.
- The documents in a folder can be signed by both participants and the initiator.
- Invisible signatures, signatures with signature images and paraphs can be used.
- Participants can be automatically reminded to sign a folder.
- Additional password protection can be activated for internal and external participants.
- External signatures can be obtained without participants needing an account.
- Signed documents can be automatically made available to all participants.
- All of a user's folders can be viewed in the dashboard and can be filtered and sorted.
- The activity history of a folder is displayed in a log.
- Templates can be used to save, manage and reuse individual settings for signature processes.
- In the user settings, the user can manage signature images, change the design and check the status of the approved signature levels.

3 Integration options:

d.velop sign is a standalone application that can be seamlessly integrated into any system via a rest interface (REST API). It has standard interfaces to d.velop documents, Power Automate, Microsoft Word and SAP (partner solution).

4 d.velop cloud Platform Apps Used

d.velop sign uses the following platform apps in addition to the basic d.velop platform apps (see "Product Description d.velop cloud platform"):

- App-router – For forwarding requests
- Billing-app – for biling
- d.velop documents – for archiving (only if this has been actively booked and linked)
- idp / uma / upa – for user connection

5 Deletion of Data

Data is deleted in accordance with the provisions of the d.velop cloud platform (see "Product Description d.velop cloud platform").

In addition, a regular deletion cycle has been established for d.velop sign to meet the obligations arising from the GDPR. Documents that users have uploaded to their d.velop sign application and that have been there for more than one year since the upload will be automatically deleted from d.velop sign. This applies

to both signed and unsigned documents. As a result, documents older than one year are no longer displayed in d.velop sign and can no longer be retrieved. They are also no longer available in the backup.

Templates created by the user are excluded from this. As templates are intended for permanent availability, they are not automatically deleted after one year. It is therefore advisable not to save any documents with personal data in these templates. However, templates can be deleted manually and irrevocably by the user at any time.

6 Information security and Privacy

The security of data is ensured by a range of technical and organizational measures that are equivalent to those for the d.velop cloud platform (see "Product Description d.velop cloud platform").

When the "sign-me" service is used, d.velop transfers personal data to D-TRUST GmbH. The purposes and means of processing are determined by D-TRUST GmbH. This therefore does not constitute data processing on d.velop's behalf. The documents are encrypted by default. XTS-AES-256 is used as the encryption algorithm.

7 Backup und Disaster Recovery

d.velop regularly backs up the contents of the d.velop cloud platform Basis Apps.

- The backups are created at least once a day, depending on the technical possibilities. The recovery point objective (RPO) is 24 hours.
- The retention time of the backups is 30 days
- Disaster recovery tests are carried out every six months.

Further information can be found in the service description of the d.velop cloud platform.