d-trust.

Secure transmission of sensitive data

Personal certificates

Advantages at a glance

01
Trusted
years of experience as an accredited German trust service provider

02
Secure
qualified trust services with the highest standards according to eIDAS

03
Reliable
application, verification and support from a single source

04
Compliant
information security management accredited according to ISO 27001

No matter what kind of digital communication, the more sensitive the contents, the greater the demands placed on data security

Create a sense of security for your business partners, customers and employees by signing and encrypting e-mails and documents with sensitive content before sending. D-Trust, Bundesdruckerei-Group's qualified trust service provider, supplies high-quality, advanced personal certificates that show the person at the other end who actually sent the message and if they really are who they claim to be. This also ensures the integrity of the information transmitted and that it can only be read by the authorized recipient. For this purpose, D-Trust issues an individual certificate for each key pair. This certificate is automatically linked to the identity of the holder.

Part of Bundesdruckerei group

bdr.

Whether economic espionage or skimming: E-mails are often gateways for cyber attacks. Furthermore, the new general data protection regulation obligates companies to prevent the abuse of customer and employee data.

Possible applications for personal certificates

Personal certificates for encrypting and signing e-mails

The Advanced Personal ID, Enterprise ID and Team ID products are primarily used to sign and encrypt e-mails. The certificate in the Personal ID and Enterprise ID products generally include the name and e-mail address of a natural person. In the case of the Enterprise ID product, the organization is also included and reference to a legal entity is established. The Team ID product, on the other hand, is used to secure e-mail communications of group mailboxes, such as sales@co.com. Besides the e-mail address, this certificate only contains details of an organization and a department.

Secure data exchange between professional secrecies

As a specialist for secure identities, D-Trust also supplies personal certificates which are issues in accordance with the technical guideline TR-03145 certified by the Federal Office for Security and Information Technology (BSI). A solution for companies, authorities and classified institutions „classified information - for official use only".

Use as a gateway certificate

All personal certificates for securing e-mail communications can also be used on e-mail gateways, in other words, as a gateway certificate. To do this, the certificate is installed on the company's e-mail gateway server. All e-mails that pass through this server can then be automatically signed with an advanced digital signature and encrypted.

Client authentication

The certificates can also be used for two-factor authentication. As soon as a server has been set up for authentication using certificates, access will then be restricted to users with the correct certificate

Document signature

Our personal certificates enable advanced electronic signatures to be attached to documents. This ensures the authenticity and integrity of the document and that a later modification does not go unnoticed.

Possible procurement channels for certificates

The certificates offered can be procured via a single request channel or D-Trust's Certificate Service Manager (CSM), a managed PKI platform. The Team ID is only available via the CSM. The CSM provides an interface for integration into legacy systems or infrastructures.

An Overview of the Functions of Personal Certificates

Functions	Personal ID	Enterprise ID	Team ID
E-mail address of a person	✔	✔	
E-mail address of a group			✔
E-mail encryption	✔	✔	✔
E-mail signature	✔	✔	✔
Organization entry	✔	✔	✔
Document signature	✔	✔	✔
Client authentication	✔	✔	✔