



**De-Mail**

# Functions and technical details

## 1. Background

The importance of the Internet has grown significantly. E-mail has now become a means of mass communication. But this supposedly simple and limitless communication per e-mail does, however, also pose challenges. It requires very little effort to intercept e-mails on the Internet and to manipulate their contents. Senders and recipients can never be really certain as to who they are in fact communicating with.

The solutions to date designed to warrant the authenticity, integrity and confidentiality of electronic communications frequently rely on end-to-end security. Such solutions are based on signature technologies – i.e. the sender signs and/or encrypts his message, the recipient decrypts it and checks the sender's signature. This, however, requires the matching software and hardware components, management of the pertinent certificates, correct interpretation of the check results, etc. Due to the level of complexity involved, solutions of this kind have not become very widespread.

In order to enable nationwide, secure online communications, the main security mechanisms of trustworthy providers who have been screened on the basis of a government-defined accreditation process are taken up in De-Mail. Before commencing work as a De-Mail provider, these providers must demonstrate that they fulfil the required functionality and IT security and that they comply with the relevant data protection requirements.

In addition to warranting the integrity and confidentiality of the messages exchanged, the main goal is to ensure the traceability of electronic communications and the authenticity of messages on the basis of known and understandable technology. That's why De-Mail must be, first and foremost, user friendly and easy to use. The services are hence pretty similar to conventional e-mail communications and should be intuitive to use.

## 2. De-Mail services

The De-Mail mailbox and delivery service is the central means of reliable and confidential communications.

De-Mail is supplemented by trustworthy document filing (De-safe) and reliable verifications of identity (De-Ident).

### ***2.1. The De-Mail mailbox and delivery service***

The central De-Mail service is to enable citizens, businesses and the administration to exchange information reliably and confidentially. Secure communication is mainly based on mutually authenticated and encrypted communication channels.

All the data which the user passes on to the De-Mail service for transmission or filing is immediately encrypted and integrity-protected.



**De-Mail**

## Functions and technical details

De-Mail offers different types of transmission which can also be used independent of each other.

- *De-Mail*: This type of transmission prevents any loss of confidentiality and any manipulation of the message text or the metadata.
- *Registered De-Mail*: The sender additionally receives confirmation with a qualified signature, stating when the message was sent and when it was delivered to the recipient's mailbox.

A user can also select one of the following options before sending a De-Mail:

- *Personal*: This option means that the recipient's level of authentication must be at least "high" (e.g. due to the confidentiality of the message) in order to be able to read the message (refer to section 3 for the different levels of authentication).
- *Sender confirmed*: After receiving the message, the sender's De-Mail provider confirms, by way of a qualified signature, receipt of the message text from the sender whose level of authenticity was at least "high". This confirmation thus provides the recipient with greater proof of the authenticity of the sender and the integrity of the messages.

Senders can also additionally sign their messages using their own components (qualified) and/or encrypt them end-to-end. De-Mail providers are obliged to offer a repository service in which users can also store encryption certificates for their De-Mail addresses.

Both individuals and legal entities can open De-Mail accounts:

Users have to be reliably identified once in order to open a De-Mail account. Individuals registering for the first time must provide mandatory data, such as first and last name, registered address and date of birth. In the case of legal entities, i.e. companies, organisations or public agencies, data concerning the legal entity itself is recorded along with information about authorised individuals.

Since reliable initial registration is vital to the required identification of the communication partners, only methods which meet the high security requirements are accepted, such as the future electronic ID card or the Post-Ident method. These security requirements are somewhat similar to the requirements when applying for a qualified signature card or opening a bank account.

One or more De-Mail addresses are assigned to each De-Mail account. These De-Mail addresses are like normal e-mail addresses only that they have the special ".De-Mail.de" extension. The address of an individual is hence made up as follows:

<firstname>.<lastname>@<De-Mailprovider>.De-Mail.de. If a name appears more than once at a De-Mail provider, a number is added to the address. A De-Mail address could hence be as follows: erika.mustermann@provider-XYZ.De-Mail.de.



**De-Mail**

## Functions and technical details

In addition to this address, a user can also create another, user-defined pseudonym De-Mail address for his account. Such addresses have a pn\_ prefix that identifies them as pseudonyms, so that such an address could be for instance: pn\_mickeymouse@provider-XYZ.De-Mail.de.

Legal entities obtain a domain as their namespace: <domain-name>.De-Mail.de. For instance, the company "Roofer Müller" could reserve the De-Mail subdomain: "roofer-mueller.De-Mail.de". The local part of the De-Mail address, i.e. the part in front of the @, can, in principle, be freely selected by the legal entity. This means that the legal entity can set up organisation mailboxes or individual mailboxes with the names of employees.

### **2.2. De-Ident**

Within the scope of De-Mail services, an easy possibility will be provided to prove identity attributes. When requested by the user, the De-Mail provider generates confirmation of identity which is then sent via De-Mail to the recipient's De-Mail address. This is to enable citizens, for instance, to register at online shops or to prove that they are over the age of 18. The De-Mail provider attaches a qualified signature to these contents, thus confirming that the data transmitted is correct.

### **2.3. De-Safe**

The safe storage of important documents in electronic form is often necessary. In this case, De-Mail providers are to provide so-called document safes in which documents can be stored over long periods of time and protected against loss or manipulation. All the documents transmitted to the safe are also encrypted and their integrity is protected immediately after receipt.

## **3. Authentication levels for logging onto a De-Mail account**

In order to use the De-Mail servers, users have to log on securely to their De-Mail account. There are basically two levels of authentication foreseen: "normal" and "high":

- *Normal*: corresponds to the user name/password
- *High*: possession and knowledge (e.g. mobile phone-based methods (TAN), certain chip cards, or the future electronic ID cards as a so-called authentication token)

The level of authentication used when logging onto the account affects the further use of the De-Mail services during the session: For instance, a minimum level of authentication can be a prerequisite for access to documents in the De-Safe, to messages in the mailbox or for using certain types of transmission. The specific level of authentication is also visible to the communication partners so that they can assess the level of trustworthiness.



**De-Mail**

## **Functions and technical details**

### **4. Accredited providers**

Within the scope of accreditation by the German Federal Office For Information Security (BSI, [www.bsi.bund.de](http://www.bsi.bund.de)), De-Mail providers must demonstrate that they have implemented the technical and organisational means which, for instance, prevent unauthorised internal or external access to data.

Furthermore, they must show that the De-Mail services which they provide are interoperable (i.e. that they co-operate smoothly on a technical level with other De-Mail providers). This is important if isolated solutions are to be avoided. De-Mail providers cannot operate on the market until they have successfully completed the accreditation process. Detailed and up-to-date information about the proposed certification and accreditation procedure will be published on the BSI website.

### **5. Technical design**

#### ***5.1. Transmission security by default***

Communication between De-Mail users and their De-Mail providers as well as communication between De-Mail providers themselves is generally established through mutually authenticated and encrypted communication channels. All messages (in the case of De-Mail) and documents (in the case of De-Safe) are encrypted and integrity-protected immediately on receipt by the De-Mail provider. When the messages or documents are retrieved, the De-Mail provider decrypts them and checks their integrity. If this level of security is not sufficient for users, they can additionally encrypt their messages or documents end-to-end or attach a (qualified) signature to the contents.

#### ***5.2. Sending a message from the sender to the De-Mail provider***

If senders use a web browser to write their messages, the message text is transmitted via HTTP(S) (*Hypertext Transfer Protocol via TLS*).

If an e-mail client is used, the message is sent to the provider via SMTP (*Simple Mail Transfer Protocol*) via TLS. De-Mail providers may support other transport protocols, such as OSCI (*Online Services Computer Interface*) which is used particularly for administrative purposes.

#### ***5.3. Verification and complementation of metadata***

Immediately after receiving a message from the sender, the De-Mail provider verifies the metadata transmitted with the message. For instance, the De-Mail address stated in the message as the sender address must be assigned to the De-Mail account from which the sender sent the message. The sender's level of authentication must also be at least "high" if the De-Mail-specific "sender confirmed" send option was selected.



**De-Mail**

## **Functions and technical details**

After verifying the metadata, the message text is checked for malware. The sender's De-Mail provider then adds other metadata, e.g. the current time, and then the message including the meta data is integrity-protected and encrypted. Only after integrity protection does a message become a De-Mail with all the integrated security features.

### ***5.4. Integrity protection and encryption***

The integrity protection provided by the De-Mail provider basically comprises a checksum (hash value) of the metadata and of the message contents. In the case of messages which are sent with the "sender confirmed" option, the provider additionally attaches a qualified signature to the hash value and the signature is additionally stored in the metadata of the message. The signature confirms that the De-Mail provider has correctly captured the metadata and that he received the message contents of the sender without any changes.

Following integrity protection, the De-Mail provider encrypts the message contents for both itself or for the recipient's De-Mail provider using a hybrid procedure.

### ***5.5. Confirmation of transmission***

Immediately before transmitting the integrity-protected and encrypted message to the recipient(s), the sender's De-Mail provider issues confirmation of transmission with a qualified signature – if requested by the sender. This confirmation of transmission is delivered to the sender as a De-Mail attachment.

The confirmation of transmission contains, among other things, the hash value of the original message and the time of transmission. This means that the sender can prove that he/she sent a specific message at a specific point in time.

### ***5.6. Secure transmission of messages to De-Mail providers***

The sender's De-Mail provider sends the integrity-protected and encrypted De-Mail to the recipient's D-mail provider using SMTP via a communication channel that has been mutually authenticated and encrypted with SSL/TLS.

After receipt of the transmission-secured message, a copy of the message is temporarily decrypted and the integrity of the message or the content is checked, for instance, for malware. The provider then discards the decrypted copy of the message and files the transmission-secured message in the recipient's mailbox.

### ***5.7. Confirmation of delivery***

Immediately after a message has been filed in the recipient's mailbox, the recipient's De-Mail provider issues confirmation of delivery for the sender – if requested by the sender. The De-Mail provider attaches a qualified signature and send returns this as a De-Mail attachment.

Confirmation of delivery contains, among other things, the hash value of the original message as well as the time at which the message was filed in the recipient's mailbox. With this confirmation of delivery, the sender can prove to third parties that the recipient had access to a specific message from a specific point in time.



**De-Mail**

## **Functions and technical details**

### ***5.8. De-Mail protocols and data formats***

Two communication paths are relevant for De-Mail communication. First, there is the path between the user and his De-Mail provider and second, there is the "internal" path between two De-Mail providers.

For security reasons, communication between the user and his provider must take place via a mutually authenticated and confidential communication channel (e.g. SSL/TLS; this can also take place via OSCl transport). De-Mail providers and users can decide on the technical implementation and hence choose the transport protocol and the data formats used.

Generally speaking, senders and recipients can use different protocols / data formats and hence client applications. When it comes to client applications, De-Mail providers must at least support web browsers with HTTP(S). Furthermore, e-mail clients with SMTP can be used to send and POP3 or IMAP can be used to receive messages, in each case via a secure communication channel.

In contrast to the communication channel between the user and the De-Mail provider, the protocols and data formats between two De-Mail providers are precisely specified so that all providers can communicate with each other (interoperability).

SSL/TLS is used to protect the communication channel between two De-Mail providers. In this secure communication channel, SMTP is used to transmit the messages and the data format is standard e-mail format (*Internet Message Format*).