



**As simple as e-mail and  
as secure as postal mail**

## **E-mails are less secure than paper post and are hence not used in many business transactions**

It is not very difficult to intercept e-mails on the Internet, to read them or to change their content. Senders and recipients can never be completely sure who they are really communicating with or whether the e-mail sent has in fact arrived at the recipient. The share of SPAM (i.e. unwanted e-mails sent in huge numbers by a sender who is often very difficult or impossible to identify) in overall e-mail traffic has increased dramatically. Illegal attempts to obtain access data to e-mail accounts (phishing, identity theft) are also becoming more frequent.

All of these aspects have up to now prevented e-mail from becoming established in places where confidentiality (encrypted), reliability (confirmation of receipt) and bindingness (secured identity), all of which are important prerequisites for legally binding transactions, are vital.

## **De-Mail is the key to confidentiality, reliability and bindingness in electronic communications**

De-Mail, which takes "simple" e-mail one step further, is an easy-to-use technology that allows messages to be exchanged on the Internet in a secure, legally binding and confidential manner.

The sender and recipient of a message can be clearly identified. Send and delivery certificates can be easily issued (registered mail). De-Mails are encrypted during transport and can hence be neither intercepted nor manipulated. SPAM is effectively prevented because the sender of De-Mails is clearly known thanks to initial identification (e.g. via the Post-Ident method). Phishing and identity theft can be prevented, for instance, if the user logs on to De-Mail using the future electronic ID card or a mobile phone-based method (mobile TAN).

Thanks to these additional security functions, a large part of today's paper-based business and administration processes can be handled fully electronically with De-Mail, simply and quickly and from any location.



# As simple as e-mail and as secure as postal mail

## De-Mail is just as easy to use as e-mail

In the simplest case, citizens and businesses can use De-Mail through web applications which are used just like familiar applications from e-mail providers and do not require any additional hardware or software installation on the part of the user. Businesses and public agencies can connect to De-Mail using their existing (internal) e-mail structures or via a so-called "Gateway", so that staff can continue using existing e-mail clients.

Opening De-Mail accounts is easy for citizens, businesses or the administration. To open an account, the user must furnish reliable ID once (e.g. using the Post-Ident method or the electronic ID card). The user then logs on daily to De-Mail using a user name/password, an electronic ID card, a mobile phone-based method (mTAN) or another secure method.

De-Mail is hence as simple as e-mail and as secure as paper post



- |                |   |                     |
|----------------|---|---------------------|
| Versicherungen | ▶ | Insurance companies |
| Banken         | ▶ | Banks               |
| Bürger         | ▶ | Citizens            |
| Firmen         | ▶ | Businesses          |
| Behörden       | ▶ | Public agencies     |

## The public and private sector jointly define the framework - the private sector implements De-Mail

All the government has to do is create the framework for secure and confidential Internet communications via De-Mail. De-Mail will then be implemented in the form of concrete products or services by interested companies that will observe this framework.

The necessary specifications for security, functionality and interoperability were drawn up by the federal government together with future De-Mail providers and laid down in technical directives. The De-Mail providers will be screened within the scope of a government accreditation/certification process to ensure compliance with these directives.

De-Mail is hence the basis for a future market for secure electronic communications which is open to all certified and accredited market participants and which thus creates a nationwide yet competition-friendly infrastructure for secure electronic communications.



**As simple as e-mail and  
as secure as postal mail**

## **A large part of the cases where De-Mail can be used concerns electronic b2b- or b2c-communications**

De-Mail is not "public agency mail", as sometimes reported, instead it is an infrastructure for the secure exchange of electronic messages which is designed for citizens and businesses. The administration is another user group.

De-Mail can be used in many ways in business to communicate with:

- business partners: offers, contracts, declarations of acceptance, contract confirmation, price quotes.
- employees: employment contracts, salary statements, personnel matters.
- public agencies: tax matters, statistics reports, visa matters, procurement, application procedures.
- chambers and associations: regular reports, applications.

## **De-Mail makes Germany more attractive as a location for business**

De-Mail offers businesses in Germany a low-cost communication infrastructure for the secure and legally binding exchange of electronic messages. According to the German Insurance Association (GDV), Germany's insurance companies alone who send around 800 million letters per post every year could save many hundred million euro annually.

De-Mail hence has the active support of the high-tech association, BITKOM, the German Insurance Association (GDV) and other business associations.

The implementation of De-Mail is also competition friendly because the government only checks compliance with the requirements for IT security, functionality and interoperability within the scope of a certification process. The government itself does not provide any application/software and therefore doesn't have to implement a "mammoth project". The De-Mail services are offered by competing companies which, based on the uniform framework, can carve their own individual profiles through different brand strategies and additional offers.

## **The private sector and associations are supporting De-Mail during the De-Mail pilot project in Friedrichshafen**

De-Mail was completed far enough with the first De-Mail providers: GMX, T-Home, T-Systems and WEB.DE, so that the pilot phase was launched on 9 October 2009 in the city of Friedrichshafen at Lake Constance ([www.fn.De-Mail.de](http://www.fn.De-Mail.de)).



## As simple as e-mail and as secure as postal mail

Participants in this pilot phase are inter alia: AWD, Citibank, CosmosDirekt, EADS, Gothaer, HUK24, LVM, Sparkasse Bodensee, Volksbank Friedrichshafen, ZF and the city administration of Friedrichshafen, the Ulm Chamber of Crafts and the Bodensee/Oberschwaben Chamber of Industry and Commerce. And, of course, many citizens who can use De-Mail free of charge during the pilot phase.

To kick off the pilot phase, the first De-Mail was sent by BITKOM to Prof Zorn who 25 years ago, as one of the founding fathers of the German Internet, received the first-ever e-mail in Germany. (<http://www.bmi.bund.de/press release>).



The main aim of the pilot phase – which has been set for an initial six month period – is to identify user acceptance of De-Mail in different application areas between businesses and citizens and with and within the administration.

Any acceptance problems or difficulties in user guidance are to be quickly identified and remedied so that when real operations are launched a mature and recognised platform can be made available to all citizens, businesses and public agencies.

*Photo: BITKOM sends first De-Mail to Prof Zorn. (Source: BMI/Hans-Joachim M. Rickel)*

### **Nationwide available in the second half of 2010**

The conceptual preconditions for the certification and approval (accreditation) of De-Mail providers will be made available early in 2010.

The legal precondition for the approval is the so-called De-Mail Act (formerly the Citizen Portals Act) which was not adopted in the last legislative period due to the lack of time. The CDU and FDP parties have included the adoption of the De-Mail Act in their coalition agreements.

In light of this, the plan now is to make De-Mail available to all citizens, businesses and public agencies in the second half of 2010.



**As simple as e-mail and  
as secure as postal mail**

### **De-Mail ensures greater data protection and data security**

Only a fraction of e-mails sent today by citizens are encrypted (less than 5%). That's why the majority of e-mails (including all attachments) can be intercepted on the Internet, read like postcards and their content manipulated. Senders and recipients can never be completely sure who they are really communicating with or whether the e-mail sent has in fact arrived at the recipient.

With De-Mail, the security and confidentiality of electronic exchange can be lifted from today's nationwide very low level to a nationwide very high level. De-Mail thus provides a very important contribution towards greater data protection and data security on the Internet.

### **Other providers are welcome to act as De-Mail providers**

More than a decade after the "Internet boom", Germany still has no nationwide infrastructure available for the confidential and legally secure exchange of messages. At the same time, the support that the De-Mail project has received from existing Internet service providers (such as GMX, T-Home, T-Systems, WEB.DE, etc.), from BITKOM and from the private sector, is a clear indication that the framework already drawn up by the government for De-Mail will enable a functioning market and prevent any island or monopoly solutions.

This is why the De-Mail project will continue to work towards participation by other companies in the future De-Mail alliance. De-Mail provides sufficient space for each provider to put forward their respective strengths (trust gained with customers, hybrid letter, etc.) in order to stand out against other De-Mail providers.