BCC
www.bcchub.com

Mail encryption without certificates

Mail Management and Security.
Quick, simple and affordable with Instant Encryption.

It's Quick - Up and running within 30 minutes.
It's Simple - For sender and recipient, online or offline, on the smartphone and iPad.
It's Affordable - Much lower costs than certificate based solutions.

Today, users expect to communicate via e-mail in a safe and uncomplicated way. The requirements may differ, for example HR Management needs to protect sensitive data in their emails or Management Directors need to have their attachments encrypted. Practically, it means that the deployment of a secure messaging infrastructure might result in high costs for the organization or too much effort for the users or e-mail recipients. The classic ways of S/MIME or PGP are expensive and complicated to implement in a running productive environment.

Web based solutions are very often complicated to handle or have lots of limitations regarding the features e.g. when the https protocol is deactivated for security reasons. Locally installed solutions often need a high degree of maintenance, possible misusage and complicated handling might cause problems for the users.

The Instant Encryption Technology powered by MailProtect is designed to satisfy both, the users and the administrators by complying with data protection needs, ensuring confidential communication and providing protection against manipulation:

- ☐ No implementation of local PKI
- ☐ No software installation on the client side
- ☐ No training for the users, no helpdesk requests
- ☐ No on-going administration efforts
- ☐ No hosting provider or other third party tools

How does instant Encryption work?

E-Mail dispatch

The new generation of the password based encryption solution uses PDF or ZIP format. Generally, the email content and all attachments of outgoing emails are converted on the server and will be sent as encrypted, password protected PDF files with embedded attachments. The administrator can predefine how the encryption is to be used, flexible to the needs of the users.

For example, all emails sent by HR Management, emails with attachments or emails with a specific keyword in the subject will be encrypted automatically. Additionally, 256 bit encrypted ZIP Archives, long term archiving format PDF/A and Windows Compressed Folders DES 40 bit Encryption are available.

Password Distribution

The password required to open the encrypted email will be generated automatically and distributed to the user separately e.g. via email as inline image, via SMS or fax. The password can also be delivered to the sender of the e-mail in case he wants to distribute it to the recipient via telephone. A long term password, valid for every email sent, can be generated for each user.

For a higher security, a different password for each email can be generated as well. The password management configured by the administrator is highly automated. In case a user has forgotten the password, it can be regenerated by just clicking on a link embedded in the email and the password will be sent automatically from the server to this user.

BCC Unternehmensberatung GmbH
Frankfurter Str. 80-82, 65760 Eschborn, Germany
+49 (0)6196 64040 0, sales@bcc.de, www.bcc.de

BCC Business Collaboration Company Ltd.
Becket House, 36 Old Jewry, London, EC2R 8DD
Tel.: +44 20 3290 9224, Email: contact@bcc.biz, www.bcchub.com