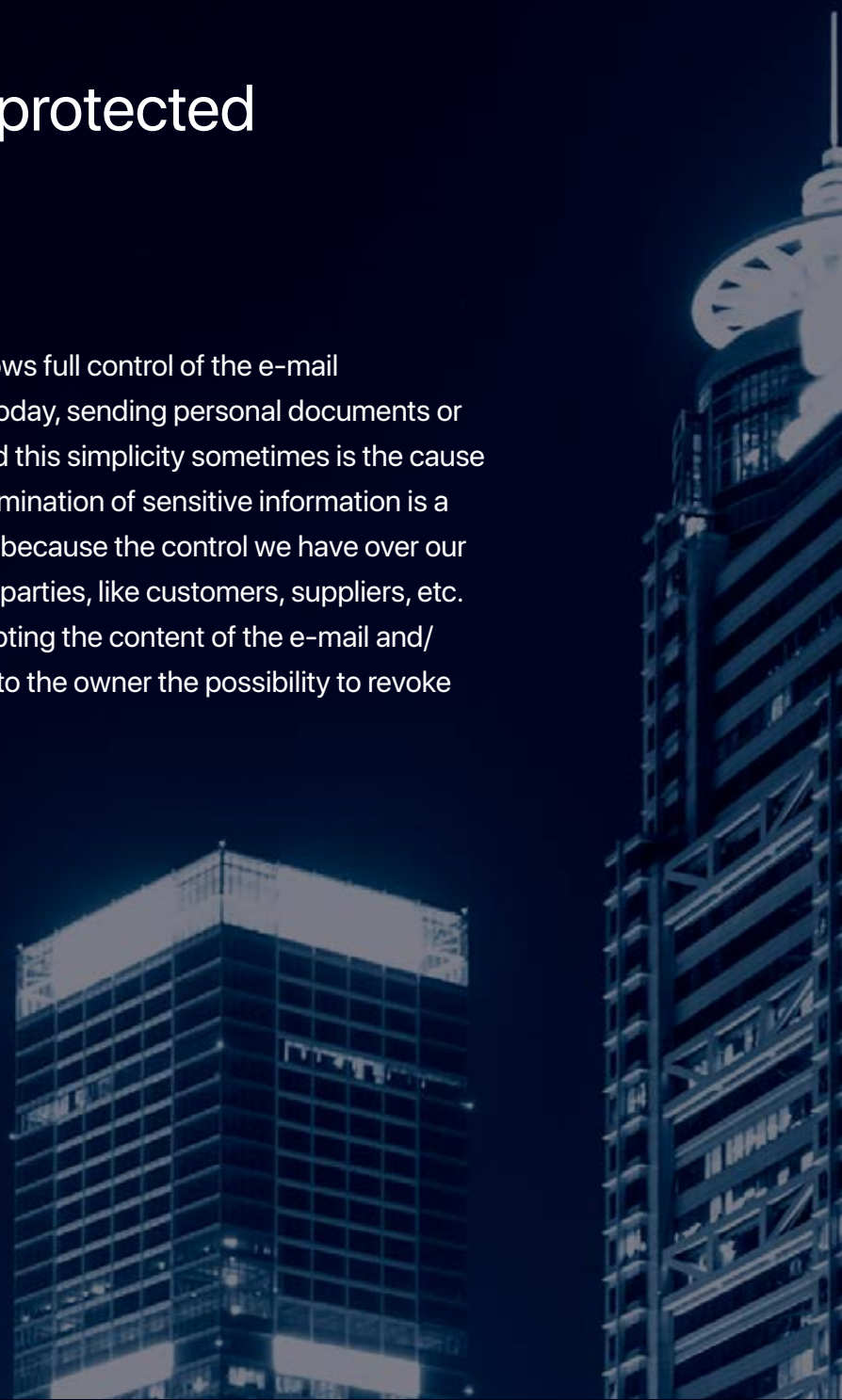
DataKrypto

DK
Mail

Your mail always protected

DK Mail

DK Mail is an Outlook plug-in that allows full control of the e-mail correspondence of an organization. Today, sending personal documents or information via e-mail is very easy and this simplicity sometimes is the cause of a data leak. The uncontrolled dissemination of sensitive information is a common problem of all organizations because the control we have over our data ends when they are sent to third parties, like customers, suppliers, etc. DK Mail solves this problem by encrypting the content of the e-mail and/or attachments (of any type), leaving to the owner the possibility to revoke access to the data at any time.



Patent pending

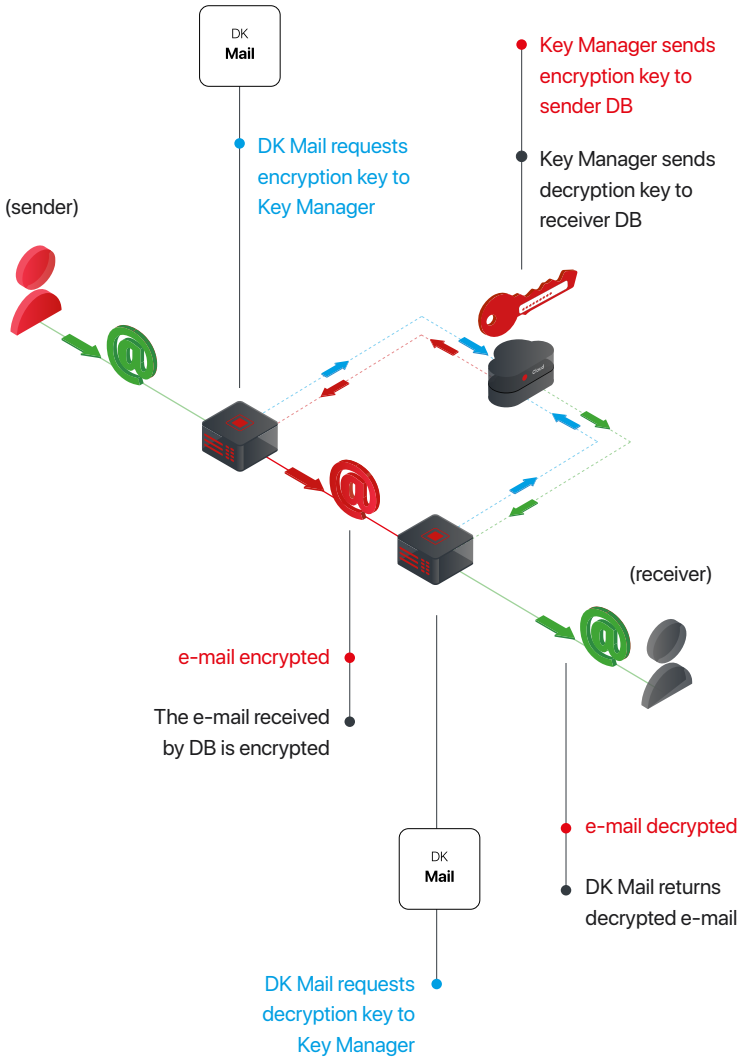
DataKrypto

How it works

DK Mail

The plug-in is installed like any other Outlook plug-in, while a Key Manager is installed within the organization.

An enrollment process in the Key Manager will generate a unique encryption / decryption key set for each user. To decrypt the content of the email, the recipient will have to request the sender's decryption key to the Key Manager. Although the Key Manager provides the decryption key only to recipients who belong to the organization, it will only be possible for sender revoke access to the email sent, making it impossible to view its content and any attachments.



DataKrypto

Use cases

DK Mail

Today the largest number of cyber attacks occur through e-mail, which is why it is necessary to take security measures on the mailboxes. Sensitive information such as social security, passwords, login credentials and bank account numbers, are vulnerable information if sent by email. DK Mail is a transversal solution for any company or public institution, capable of perform the process of masking the content of your email messages, to protect them from reading by unauthorized people.

Public sector

With DK Mail, it becomes possible avoid any form of data leak, since the process that leads to the decoding of email and attached documents necessarily implies verification of the identity of the sender. Only if the sender is really who he says he is and therefore it is registered internally of the organization as a valid user, it will be possible use his key for decrypt the data.

Enterprise

With DK Mail, it's possible to protect sensitive information independently from the location of the server mail. In this way, also of in the face of a data leak born within a managed server from third parties, no damage will be suffered whatsoever. Furthermore, DK Mail makes correspondence in accordance with GDPR, as even after having sent a document is always access can be revoked to the recipient in any moment.

Education

With DK Mail, an Active Directory is protected by preventing attackers from breaching a host through sensitive data contained within a mail account. By filtering the emails received between registered and unregistered users, a phishing email is prevented from collecting any type of personal information.

DataKrypto Company
Via Marche, 54 - 00187 Rome, Italy

www.datakrypto.com
email: info@datakrypto.com - tel. +39 06 5413047