



# Communicate securely with your clients

Solution demand for government and self-government



Security of e-mail communication



Security communication via e-mail room



Protection of personal data



Data leakage prevention

## What and with whom you communicate

### Internal communication

board members and representatives  
trade Union leaders  
employees  
personnel department

Who?  
With whom?

negotiation documents, personal data,  
financial results, payslips,  
labour law documentation, tender  
documents for public tenders

What?  
What sort of content?

### External communication

citizens  
organizations established and managed  
by the regional office, the ministry  
contribution organizations  
external lawyers and consultants, partners

strategy documents, citizens personal  
data, consultation and investment  
preparation, grant programs and  
projects, public tenders

## What solution you look for

Simple encryption of e-mails,  
files and folders on PC

Fast implementation and  
inexpensive infrastructure

Time limitation of access  
to messages

Possibility of limitation of  
sending personal data in an  
insecure way

Access denial to messages in case  
of an employee leaving or  
business partner changing

Free of charge content  
decryption by an external  
recipient without the need of  
installation or registration

Digital signature - confirmation  
of sender identity

Full user control over  
the system running

Assurance of message not  
being read by anyone other  
than the sender and the  
recipient

If you send anything by an e-mail,  
you would not write onto a postcard,  
encrypt it.



Your e-mail, as well as a postcard can be read by whoever going by.

Good day,

Please fill in the contract header  
in order to preparation:

seller...residence...  
personal identification number....

buyer...based...  
ID....



Caroline Region

Regional Street 123/4

Ostrava

7 0 2 0 0

Czech Republic

## 3 reasons why encryption with Talkey is the most safest way of e-mail communication

### 1 Guarantee your identity

Encrypted message by Talkey guarantees the origin, the authorship and the stability of a message. Your clients and partners know that they should open only encrypted e-mails received from you, which protect them from cheated message, which will misuse your company domain. You, on the other hand, know that you are taking every step possible for protecting your client's data and therefore preventing court cases, financial losses and the loss of reputation.

### 2 Be in control over the way how the recipient will treat your message

Set what the recipient can or cannot do with your message. Protect information and data sent by e-mails. For instance, you can prohibit the recipient from forwarding your message, determine how many times or how long for the message can be opened, until it is invalid and therefore impossible to decrypt.

these advanced features will help you  
with that

### 3 Take really back a wrongly sent e-mail

Do you know that, in reality, a common e-mail client can not delete an e-mail, even though you click on "take back" button? Such e-mail will stay hanging in between the servers and could be read by anybody, basically. Talkey enables to make a sent e-mail invalid, which means, that the e-mail could not be opened neither by the recipient or anyone else.



disable the recipient's ability to forwarding  
your message



set the number of times the message can  
be opened



limit the amount of time your message  
to be visible



do not allow the message to be displayed  
on mobile device