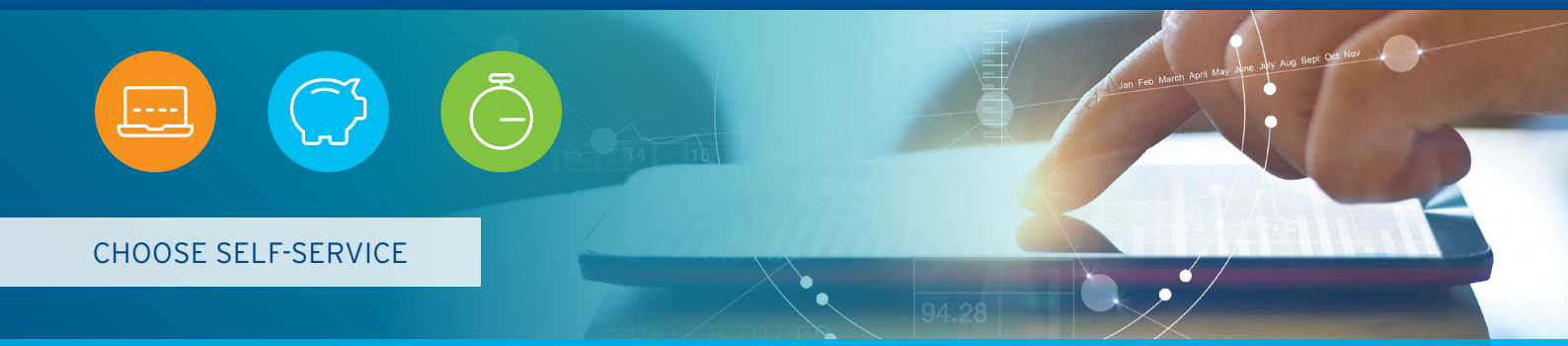
www.citihandlowy.pl
Bank Handlowy w Warszawie S.A.

150 years of progress

citi handlowy®



CHOOSE SELF-SERVICE

Secure email communication

In accordance with our security policy, we ensure that our communication with our Customers via email (especially containing confidential or proprietary content) is adequately secured. We strive to minimise the risk of potential unauthorised access or substitution of data. Therefore, we recommend that the following encryption tools be used:

SecureEmail – thanks to using this mechanism both the message itself and the attached files are encrypted. It is used to send emails containing confidential, proprietary/sensitive data, including personal data. The addressee decrypts the message using a predefined password.

MTLS – provides automatic encryption of email communication between Citi's domain and the Customer's domain. In this case, there is no need to further encrypt emails containing confidential, proprietary/sensitive data, including personal data.

Below we would like to present the differences between the selected methods of encrypting email messages.

SecureEmail	MTLS
It is mandatory that you use the word (SECURE) at the beginning of the subject of an email.	Every outgoing email to an addressee whose domain was configured as part of the MTLS method is automatically sent as encrypted.
The Addressee must complete a one-time registration process and generate a password to receive messages sent in the SecureEmail mode. The instruction regarding registration and/or downloading of an encrypted message by the Addressee will be included in the first secure email received from Citi Handlowy.	No additional action is required – the email is opened in a standard way.
The entire email, including attachments, is encrypted.	The content of the message is displayed as regular text. The entire message, including attachments, is protected during sending.
An email sent in the SecureEmail mode waits three business days to be downloaded, and when this deadline expires, it will no longer be possible to download and read it.	The MTLS encryption method can only be applied between domains configured with Citi's domain.

Implementation of safe communication – requirements:

- **Secure email** – it is important that users (message addressees) have unlocked access to external websites, because using this method requires completion of registration and setting of a permanent password (every subsequent message will be decrypted using the set password). To receive a message, the regular software Adobe Acrobat Reader version 9 or higher is required.
- **MTLS** – the requirements necessary to implement this type of encryption are as follows:
  - Use of an approved X.509v3 certificate. In the absence of this certificate, it must be purchased and installed;
  - The certified key size must be 2048 bits or higher;
  - The encryption strength of the email servers must be 256 bits or more;
  - The third party must use a private business domain for emails, such as @companyabc.com. The MTLS cannot be used for emails sent to public domains, such as @gmail.com;
  - Completion of the MTLSreqestform application.

Your CitiService Advisor will provide you with the details of the functionality and implementation of the selected email encryption methods.