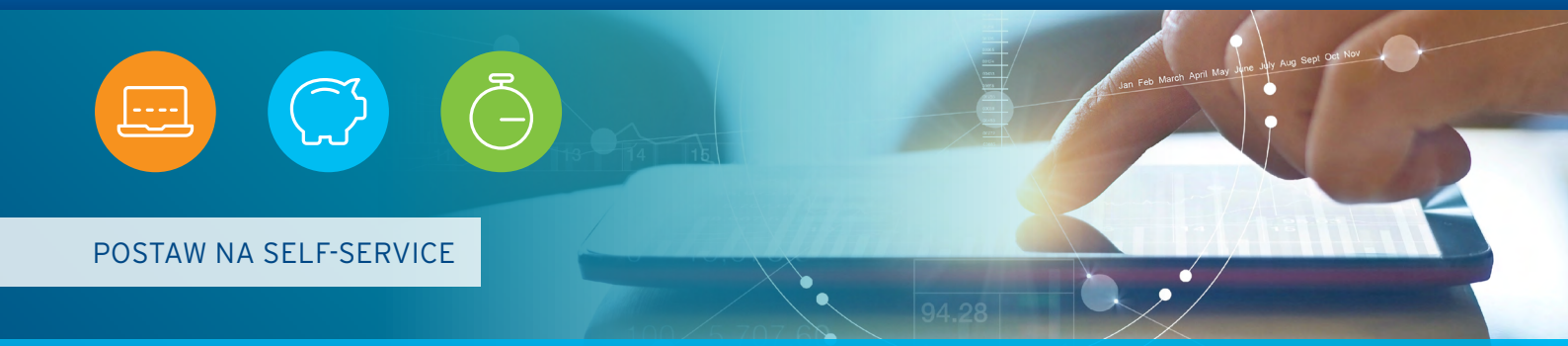

POSTAW NA SELF-SERVICE

Bezpieczna komunikacja e-mail

Zgodnie z polityką bezpieczeństwa dbamy, aby nasza komunikacja z Klientami poprzez wiadomości e-mail (zwłaszcza zawierające treści poufne lub zastrzeżone) była odpowiednio zabezpieczona. Dążymy do minimalizacji ryzyka potencjonalnego nieuprawnionego dostępu lub podmiany zawartości danych. Dlatego rekomendujemy stosowanie narzędzi szyfrujących:

SecureEmail – dzięki zastosowaniu tego mechanizmu zarówno treść wiadomości, jak i załączone pliki są szyfrowane. Stosuje się go do wysyłania wiadomości e-mail zawierających dane poufne, zastrzeżone/wrażliwe, w tym dane osobowe. Odbiorca odszyfrowuje wiadomość przy użyciu wcześniej ustalonego hasła.

MTLS – zapewnia automatyczne szyfrowanie komunikacji e-mail między domeną Citi a domeną Klienta. W tym przypadku nie ma konieczności dodatkowego szyfrowania e-maili zawierających dane poufne, zastrzeżone/wrażliwe, w tym dane osobowe.

Poniżej przedstawiamy różnice pomiędzy wyróżnionymi metodami szyfrowania wiadomości e-mail.

SecureEmail	MTLS
Obowiązkowo w temacie wiadomości e-mail na początku należy użyć słowa (SECURE).	Każdy wychodzący e-mail do odbiorcy, którego domena została skonfigurowana w ramach metody MTLS, jest automatycznie wysyłany jako szyfrowany.
Odbiorca musi ukończyć jednorazowy proces rejestracji i wygenerować hasło, by odbierać wiadomości wysłane w trybie SecureEmail. Instrukcja dotycząca rejestracji i/lub pobierania zaszyfrowanej wiadomości przez Odbiorcę będzie zawarta w pierwszej bezpiecznej wiadomości e-mail otrzymanej od Citi Handlowy.	Podejmowanie dodatkowych działań nie jest wymagane – wiadomość e-mail otwierana jest w standardowy sposób.
Szyfrowana jest cała treść wiadomości e-mail, łącznie z załącznikami.	Treść wiadomości jest wyświetlana jako tradycyjny tekst. Podczas przesyłania chroniona jest cała wiadomość, łącznie z załącznikami.
Wiadomość e-mail wysłana w trybie SecureEmail oczekuje trzy dni robocze na pobranie, po upływie tego terminu wygasa możliwość jej pobrania i odczytania.	Metoda szyfrowania MTLS może być stosowana tylko pomiędzy domenami skonfigurowanymi z domeną Citi.

Wdrożenie bezpiecznej komunikacji – wymagania:

- **Secure email** – ważne jest, by użytkownicy (odbiorcy wiadomości) mieli odblokowane dostępy do zewnętrznych stron internetowych, gdyż użycie tej metody wymaga ukończenia rejestracji i ustalenia stałego hasła (każda następna wiadomość będzie odszyfrowywana przy użyciu ustalonego hasła). By odebrać wiadomość, wymagane jest standardowe oprogramowanie Adobe Acrobat Reader w wersji 9 lub wyższej.
- **MTLS** – wymagania niezbędne do wdrożenia tego rodzaju szyfrowania są następujące:
  - Użycie zatwierdzonego certyfikatu X.509v3. W przypadku braku tego certyfikatu musi on zostać zakupiony i zainstalowany;
  - Certyfikowany rozmiar klucza musi wynosić 2048 bitów lub więcej;
  - Siła szyfrująca serwerów poczty elektronicznej musi wynosić 256 bitów lub więcej;
  - Strona zewnętrzna musi używać prywatnej domeny biznesowej dla poczty e-mail, na przykład @companyabc.com. Nie można używać MTLS do wiadomości e-mail wysyłanych do domeny publicznej, na przykład @gmail.com;
  - Wypełnienie wniosku MTLSreqestform.

Szczegółowych informacji dotyczących funkcjonalności oraz wdrożenia wyróżnionych metod szyfrowania wiadomości e-mail udzieli Państwu Doradca CitiService.