CUI - zmiany w autoryzacji

Szanowni Klienci,
w związku z wdrożeniem Payment Services Directive 2 Dyrektywy Parlamentu Europejskiego i Rady (UE) nr 2015/2366 z dnia 25 listopada 2015 roku (**PSD2**) w sprawie usług płatniczych w ramach rynku wewnętrznego od dnia **14 września 2019** roku będziemy zmuszeni zablokować możliwość autoryzowania transakcji przy pomocy Tokena, co będzie równoznaczne z brakiem możliwości autoryzacji dyspozycji **i brakiem dostępu do bankowości elektronicznej przez Klientów, którzy logują się przy pomocy Tokena**.

PSD2 nakłada na banki obowiązek wzmocnienia bezpieczeństwa autoryzacji transakcji, tzw. silne uwierzytelnienie klienta. Aby zainicjować płatność konieczna będzie identyfikacja Klienta za pomocą co najmniej 2 niezależnych metod uwierzytelnienia.

Dostosowując się do nowych obowiązków w zakresie silnego uwierzytelnienia, Bank udostępnił metodę autoryzacji przy wykorzystaniu następujących urządzeń autentykacji i autoryzacji:

TOKEN MMA
1. Proces autentykacji
a) Brak sparowanego urządzenia mobilnego. Po wywołaniu strony do logowania użytkownik wprowadza swój identyfikator alfanumeryczny w polu [Numer Identyfikacyjny]. Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia hasła maskowanego. Wymagane jest podanie losowo wybranych pozycji z hasła, pozostałe znaki z hasła są ukryte. Jako kolejny krok rozpoczyna się proces parowania urządzenia. Po wyborze przycisku [POSIADAM APLIKACJĘ] zostanie wyświetlona formatka z drugim krokiem procesu, na której prezentowany jest kod aktywacyjny, który należy wprowadzić w aplikacji mobilnej Asseco MAA podczas rejestracji urządzenia. Pasek postępu odlicza czas pozostały na parowanie. Proces parowania wymaga wprowadzenia otrzymanego kodu SMS oraz samodzielnego ustalenia kodu PIN do aplikacji Asseco MAA. Po sparowaniu urządzenia w aplikacji mobilnej Asseco MAA i systemie bankowości internetowej prezentowane jest potwierdzenie poprawnego parowania. Na sparowane urządzenie zostaje wysłane powiadomienie PUSH z informacją o autoryzacji logowania do systemu. Po wyborze banera powiadomienia PUSH system operacyjny przenosi użytkownika do aplikacji Asseco MAA. Wymagane jest zalogowanie do aplikacji Asseco MAA kodem PIN ustawionym podczas rejestracji urządzenia. Po zalogowaniu do aplikacji Asseco MAA na liście autoryzacji znajduje się nowa, aktywna autoryzacja. Po wybraniu autoryzacji zostają wyświetlone jej szczegóły autoryzacji oraz możliwość Odrzucenia lub Akceptacji autoryzacji. Akceptacja autoryzacji wymaga wprowadzenia kodu PIN ustawionego podczas rejestracji urządzenia. Poprawne wprowadzenie kodu PIN kończy proces logowania użytkownika do systemu bankowości internetowej.

b) Sparowane urządzenie mobilne. Po wywołaniu strony do logowania użytkownik wprowadza swój identyfikator alfanumeryczny w polu [Numer Identyfikacyjny]. Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia hasła maskowanego. Wymagane jest podanie losowo wybranych pozycji z hasła, pozostałe znaki z hasła są ukryte. Po wybraniu [ZALOGUJ] zostaje wyświetlony komunikat informujący o konieczności potwierdzenia logowania za pomocą aplikacji Asseco MAA zainstalowanej na sparowanym urządzeniu. Na sparowane urządzenie zostaje wysłane powiadomienie PUSH z informacją o autoryzacji logowania do systemu. Po wyborze banera powiadomienia PUSH system operacyjny przenosi użytkownika do aplikacji Asseco MAA. Wymagane jest zalogowanie do aplikacji Asseco MAA kodem PIN ustawionym podczas rejestracji urządzenia. Po zalogowaniu do aplikacji Asseco MAA na liście autoryzacji znajduje się nowa aktywna autoryzacja. Po wybraniu autoryzacji zostają wyświetlone jej szczegóły autoryzacji oraz możliwość Odrzucenia lub Akceptacji autoryzacji. Akceptacja autoryzacji wymaga wprowadzenia kodu PIN ustawionego podczas rejestracji urządzenia. Poprawne wprowadzenie kodu PIN kończy proces logowania użytkownika do systemu bankowości internetowej.
2. Proces autoryzacji Użytkownik wybiera opcję autoryzacji dyspozycji w bankowości internetowej i system prezentuje ekran informujący o wysłaniu dyspozycji do autoryzacji na aplikację mobilną Asseco MAA. W tym samym czasie wysyłane jest do aplikacji mobilnej powiadomienie PUSH o nowej dyspozycji do autoryzacji. Asseco MAA wyświetla na urządzeniu mobilnym baner powiadomienia PUSH z informacją o oczekującym powiadomieniu autoryzacyjnym. Użytkownik wybiera baner powiadomienia PUSH, który uruchamia aplikację Asseco MAA. W kolejnym kroku należy zalogować się do Asseco MAA za pomocą kodu PIN zdefiniowanego przez użytkownika w procesie rejestracji urządzenia autoryzującego. Aplikacja mobilna Asseco MAA prezentuje dane dyspozycji do autoryzacji wraz z możliwymi przyciskami [ODRZUĆ] oraz [AKCEPTUJ]. Dodatkowo Asseco MAA prezentuje czas jaki pozostał do potwierdzenia autoryzacji, po upływie którego dyspozycja jest anulowana. W przypadku podjęcia przez użytkownika decyzji o akceptacji dyspozycji, użytkownik weryfikuje wprowadzone dane oraz potwierdza realizację dyspozycji poprzez wprowadzenie poprawnego kodu PIN (zdefiniowanego przez użytkownika w procesie rejestracji urządzenia autoryzującego) oraz wybór przycisku [ZATWIERDŹ]. Zarówno Asseco MAA jak i system bankowości internetowej prezentuje potwierdzenie autoryzacji dyspozycji.

KOD SMS

1. Proces autentykacji
Po wywołaniu strony do logowania użytkownik wprowadza swój identyfikator alfanumeryczny w polu [Numer Identyfikacyjny]. Po użyciu przycisku [DALEJ] wyświetlane jest okno służące do wprowadzenia hasła maskowanego. Po wyborze przycisku [DALEJ], system bankowości internetowej poprosi o podanie kodu SMS wysłanego na wskazany nr telefonu. Pozytywna weryfikacja przez system podanych danych pozwoli na zalogowanie się użytkownika i wyświetlenie ekranu startowego. Negatywna weryfikacja przez system spowoduje wyświetlenie komunikatu o konieczności powrotu do procesu logowania.
2. Proces autoryzacji
Użytkownik wybiera opcję autoryzacji dyspozycji w bankowości internetowej. System bankowości internetowej prezentuje ekran z polem autoryzacyjnym - hasło wykorzystywane w procesie logowania i kod SMS. Poprawne podanie danych i wybór przycisku [AKCEPTUJ] spowoduje przekazanie operacji do realizacji.

KARTA MIKROPROCESOROWA I APLIKACJA SCSA

1. Proces autentykacji
Proces autentykacji wymaga uruchomienia aplikacji SCSA na komputerze użytkownika bankowości internetowej (w/w aplikację można uruchomić podczas procesu autentykacji do systemu bankowości internetowej) oraz umieszczenia karty mikroprocesorowej w czytniku. Na formatce logowania użytkownik bankowości wprowadzi swój identyfikator (login) a następnie wybierze przycisk [URUCHOM APLIKACJĘ] w celu uruchomiona SCSA (jeśli SCSA jest już uruchomione to następuje wywołanie aplikacji SCSA w celu wprowadzenia kodu PIN-u). W kolejnym kroku zaprezentowany zostanie ekran, na którym należy wprowadzić poprawny kod PIN potwierdzający zalogowanie do SCSA i systemu bankowości internetowej. Po wprowadzeniu prawidłowej wartości kodu PIN w aplikacji SCSA pojawi się potwierdzenie poprawnego logowania.
2. Proces autoryzacji
Proces autoryzacji (podobnie jak i autentykacji) wymaga uruchomienia aplikacji SCSA na komputerze użytkownika bankowości oraz umieszczenia karty mikroprocesorowej w czytniku. Na ekranie akceptowanego zlecenia udostępniona zostanie sekcja umożliwiająca złożenie podpisu za pomocą aplikacji SCSA. Wybór przycisku [PODPISZ] na formatce realizacji zlecenia spowoduje: - wyświetlenie oczekiwania na złożenie autoryzacji na formatce akceptowanego zlecenia, - wyświetlenie szczegółów zlecenia i pola do uzupełnienia kodu PIN-u do karty mikroprocesorowej w aplikacji SCSA. Wprowadzenie prawidłowej wartości kodu PIN i

wybór przycisku [PODPISZ] w SCSA kończy proces autoryzacji zlecenia.
W związku z powyższym prosimy, by w trakcie najbliższej wizyty w Banku (lecz nie później niż do dnia 14 września 2019 r.) złożyć wniosek o zmianę sposobu autoryzacji na mToken Asseco MAA lub SMS autoryzacyjny. Nadmieniamy, że aktywacja i użytkowanie Tokena Asseco MAA są bezpłatne.
Klientów wykorzystujących do logowania do bankowości internetowej sprzętowe tokeny prosimy dodatkowo o uzyskanie w Placówce Banku zmiany sposobu logowania przy wykorzystaniu hasła maskowanego.

Szczegółowe informacje dotyczące Tokena mogą Państwo uzyskać w Placówkach Banku oraz pod adresem strony: www.tokenmobilny.pl