



**Dostosowanie  
środków dostępu użytkowanych  
w systemach bankowości elektronicznej  
detailed Asseco CBP wymagań SCA  
(silne uwierzytelnianie)**

## 1. Wstęp – dostosowanie środków dostępu użytkowanych w CUI do wymogów silnego uwierzytelniania (SCA)

Obecnie stosowane środki dostępu do systemów bankowości elektronicznej zostały uzupełnione o dodatkowe wymagania SCA (tzw.: „silne uwierzytelnienie klienta”). „Silne uwierzytelnianie klienta” oznacza uwierzytelnianie w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii: wiedza (coś, co wie wyłącznie użytkownik), posiadanie (coś, co posiada wyłącznie użytkownik) i cechy klienta (coś, czym jest użytkownik), niezależnych w tym sensie, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych, które to uwierzytelnianie jest zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających.

Dostosowanie do wymogów SCA dotyczy procesu autentykacji (logowania) oraz autoryzacji (podpisu).

W/w zasada (SCA) determinuje zmiany w obecnie użytkowanych schematach środków dostępu, tj.:

### Bankowość detaliczna – Asseco CBP

- autentykacja: hasło maskowane, autoryzacja: kod SMS
- autentykacja: hasło maskowane, autoryzacja: token mobilny Asseco MAA
- autentykacja: hasło stałe + token RSA, autoryzacja: hasło stałe + token RSA
- autentykacja: hasło maskowane, autoryzacja: token RSA

## 2. Asseco CBP – dostosowanie do wymagań SCA

Środki dostępu w bankowości detalicznej będą dostosowane do SCA zgodnie ze schematami przedstawionymi w tabeli 1:

Tabela 1	Przed wprowadzeniem SCA		Po wprowadzeniu SCA	
Nr schematu „autentykacja - autoryzacja”	Obecna autentykacja	Obecna autoryzacja	Nowa autentykacja	Nowa autoryzacja
1	Hasło maskowane	Kod SMS	Hasło maskowane + kod SMS	Kod SMS + PIN
2	Hasło maskowane	Token mobilny Asseco MAA	Hasło maskowane + token mobilny Asseco MAA + PIN	Token mobilny Asseco MAA + PIN
3	Hasło stałe + token RSA	Hasło stałe + token RSA	Hasło maskowane + kod SMS	Kod SMS + PIN
			Hasło maskowane + token mobilny Asseco MAA + PIN	Token mobilny Asseco MAA + PIN
			Hasło maskowane + token mobilny Asseco MAA + PIN	Token mobilny Asseco MAA + PIN
4	Hasło maskowane	Hasło stałe + token RSA	Hasło maskowane + kod SMS	Kod SMS + PIN
			Hasło maskowane + token mobilny Asseco MAA + PIN	Token mobilny Asseco MAA + PIN

### 2.1. Opis szczegółowy – schemat nr 1 (dostosowanie do SCA środka dostępu – autentykacja: Hasło maskowane, autoryzacja: Kod SMS)

a) Wygląd formatek dla użytkownika po wprowadzeniu SCA

i) **autentykacja:**

Wprowadzenie identyfikatora użytkownika:


## Wprowadzenie hasła maskowanego:

### LOGOWANIE

Kod dostępu

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		*		*	*		+	+	*	+	+	+	+	+	*	+	+	*	+	+	+	+	+

**DALEJ**

 Pamiętaj o podstawowych zasadach bezpieczeństwa.

Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenia internetowe)
- w pasku adresu lub na pasku statusu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigCert Inc

Pamiętaj! Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#).

## Wprowadzenie kodu SMS:


### LOGOWANIE

Kod dostępu

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*

Kod SMS:

**ZALOGUJ**

 Pamiętaj o podstawowych zasadach bezpieczeństwa.

Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:

- adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)
- w pasku adresu lub na pasku statusu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- po kliknięciu w kłódkę pojawi się certyfikat wystawiony dla Centrum Usług Internetowych przez firmę DigCert Inc

Pamiętaj! Bank nie wymaga potwierdzenia danych SMS-em lub mailem.

Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: [Zasady bezpieczeństwa](#).

## ii) autoryzacja:

Pierwsza autoryzacja będzie poprzedzona wysłaniem poprzez SMS jednorazowego numeru PIN wraz z wymuszeniem jego zmiany:

← Przelew ×

ZWYKŁY

Przelew z rachunku	Rachunki Bieżące 84 8707 0006 0000 5656 2000 0001
Odbiorca	Jan Testowy
Rachunek odbiorcy	02 1500 1894 0690 2900 3640 4254 KBSA O. w Chorzowie
<b>Kwota</b>	<b>1,43 PLN</b>
Tytułem	tytuł testowy
Data realizacji	dzisiaj 26.08.2019

↓ Pokaż dodatkowe informacje

Wymagana zmiana pinu autoryzacyjnego

Prosimy pamiętać, że pin autoryzacyjny jest numerem poufnym. W związku z tym nie powinien być ujawniany osobom trzecim. Definiując swój pin autoryzacyjny pamiętaj o zachowaniu podstawowych zasad bezpieczeństwa:

Pin Autoryzacyjny:  
musi składać się z 4-znaków  
musi się różnić od 3 ostatnich pinów

Obecny pin autoryzacyjny	<input type="text" value="Wpisz obecny pin"/>
Nowy pin autoryzacyjny	<input type="text" value="Wpisz nowy pin"/>
Powtórz nowy pin	<input type="text" value="Powtórz nowy pin"/>

**ZATWIERDŹ**

Kolejne autoryzacje będą wymagały wprowadzenia zdefiniowanego wcześniej PIN-u do podpisu oraz kodu SMS:

← Przelew ×

ZWYKŁY

Przelew z rachunku	Rachunki Bieżące 84 8707 0006 0000 5656 2000 0001
Odbiorca	ODBIORCA SKROCONY PEŁNY
Rachunek odbiorcy	94 1020 1505 0000 0802 0011 2714 PKOBP
<b>Kwota</b>	<b>1,00 PLN</b>
Tytułem	TYTUŁ PŁATNOŚCI
Data realizacji	dzisiaj 26.08.2019
↓ Pokaż dodatkowe informacje	
Pin autoryzacyjny oraz kod SMS	<input type="text" value="Wpisz pin"/>
	<input type="text" value="Wprowadź kod"/>
	Operacja nr 738167 z dnia 26.08.2019

**AKCEPTUJ**

2.2. Opis szczegółowy - schemat nr 2 (dostosowanie do SCA środka dostępu – autentykacja: Hasło maskowane, autoryzacja: Token mobilny Asseco MAA)

a) Wygląd formatek dla użytkownika

i) **autentykacja:**

Wprowadzenie identyfikatora użytkownika:

The screenshot shows a login page titled "LOGOWANIE". At the top right, there is a language selector set to "PL". The main content area contains a form with two input fields: "Numer Identyfikacyjny" and "Kod dostępu". Below the fields is a blue "DALEJ" button. Underneath the button, there is a lock icon and the text "Pamiętaj o podstawowych zasadach bezpieczeństwa". Below this, there is a list of instructions: "Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy:" followed by three bullet points: "adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe)", "w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka", and "Pamiętaj! Bank nie wymaga potwierdzenia danych SMS-em lub mailem". At the bottom, there is a link: "Więcej informacji na temat bezpieczeństwa znajdziesz na stronie: Zasady bezpieczeństwa".

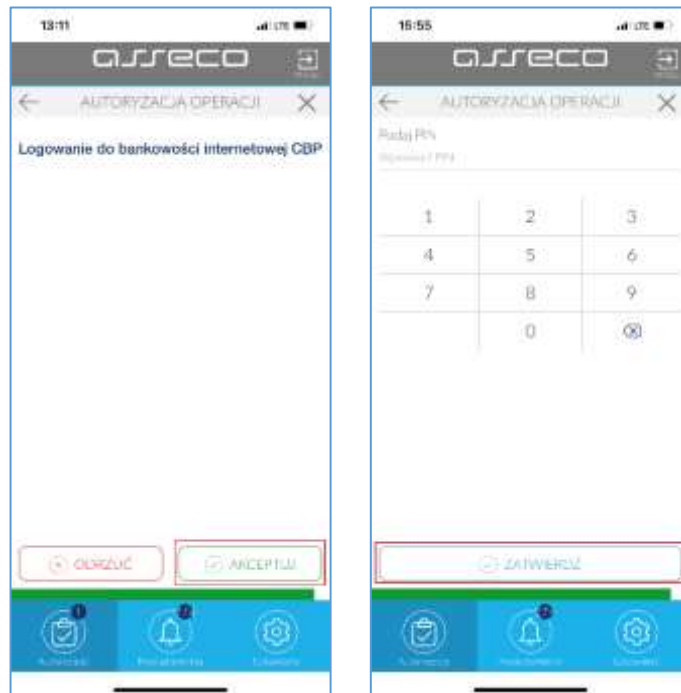
Wprowadzenie hasła maskowanego:

The screenshot shows the same login page "LOGOWANIE". The "Kod dostępu" field is now a numeric keypad with 24 positions, numbered 1 to 24. The "DALEJ" button is still present. The security instructions are the same as in the previous screenshot, including the list of checks and the link to security rules.

Oczekiwanie na potwierdzenie logowania tokenem mobilnym Asseco MAA:

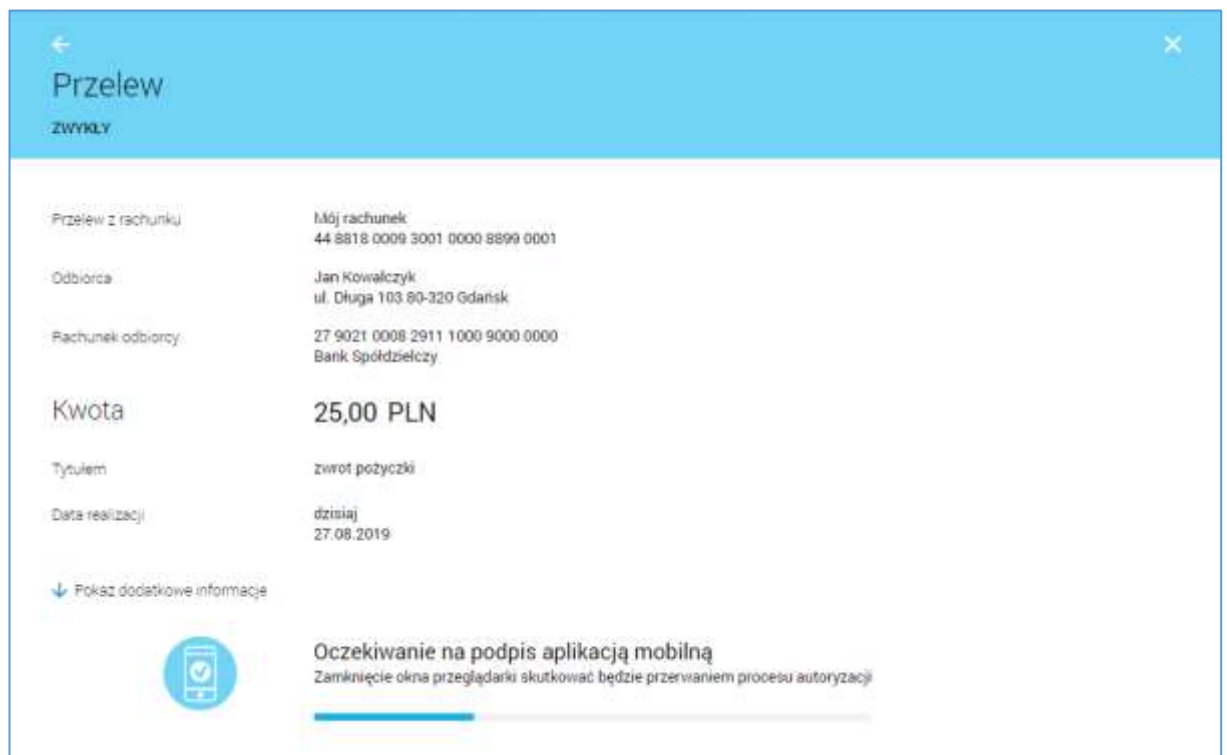
The screenshot shows a page titled "Uwierzytelnianie". In the center, there is a circular logo with a blue and yellow design. To the right of the logo, the text reads: "Oczekiwanie na uwierzytelnienie aplikacją mobilną" and "Zamknij ekran przeglądarki i uruchom aplikację mobilną, aby potwierdzić proces logowania". Below the text is a progress bar that is partially filled with blue.

Akceptacja w tokenie mobilnym Asseco MAA jest ostatnim krokiem logowania do systemu:



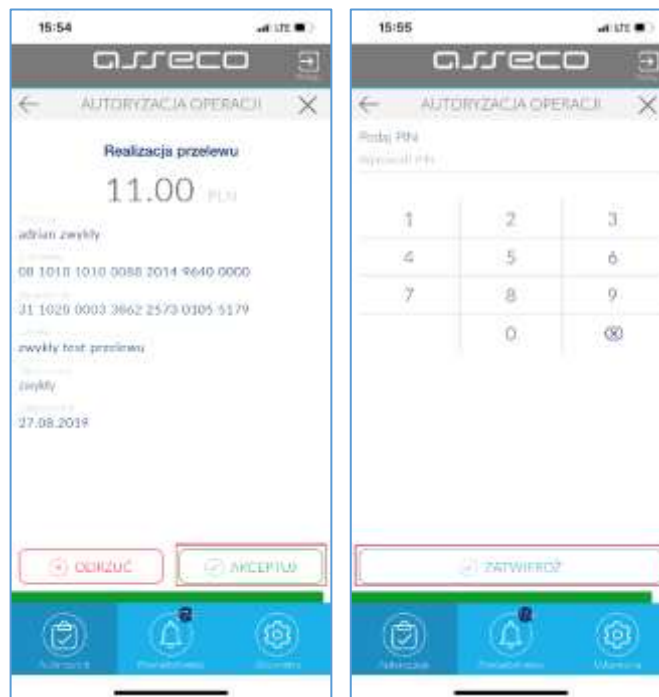
ii) **autoryzacja:**

Oczekiwanie na potwierdzenie autoryzacji tokenem mobilnym Asseco MAA:





Akceptacja w tokenie mobilnym Asseco MAA jest ostatnim krokiem w procesie autoryzacji:



2.3. Opis szczegółowy – schemat nr 3 (dostosowanie do SCA środka dostępu – autentykacja: Hasło stałe + Token RSA, autoryzacja: Hasło stałe + Token RSA)

Zmiana metody autentykacji realizowana będzie w wariantach bez zmiany identyfikatora Klienta:

- i) Pozyskanie numeru telefonu od Klienta
- ii) Zmiana metody autentykacji na hasło maskowane.
- iii) Przypisanie jednego ze środków dostępu:
  - Autentykacja: hasło maskowane + kod SMS, autoryzacja: PIN + kod SMS
  - Autentykacja: hasło maskowane + token mobilny Asseco MAA + PIN, autoryzacja: token mobilny Asseco MAA + PIN
- iv) Przekazanie Klientowi hasła.