

Zmiany w bankowości w obrębie użytkownika tokenów VASCO

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

Obecnie stosowane środki dostępu do systemów bankowości elektronicznej zostaną 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).

Planowanie termin wprowadzenia zmian to 11.09.2019 r, lecz nie później niż 14.09.2019r.

2. Tokeny VASCO – dostosowanie do wymagań SCA

Środki dostępu w bankowości korporacyjnej będą dostosowane do SCA zgodnie ze schematami przedstawionymi w poniższej tabeli:

Nr schematu „autentykacja - autoryzacja”	Przed wprowadzeniem SCA		Po wprowadzeniu SCA	
	Obecna autentykacja	Obecna autoryzacja	Nowa autentykacja	Nowa autoryzacja
1	Hasło stałe + token VASCO DP260	Token VASCO DP260 + PIN	Hasło stałe + token VASCO DP260 + PIN	Token mobilny Asseco MAA + PIN (mToken)
2	Hasło stałe + token VASCO DP260	Token VASCO DP260 + PIN	Hasło stałe + token VASCO DP260 + PIN	Karta mikroprocesorowa (aplikacja SCSA) + PIN

2.1 Opis szczegółowy - Hasło stałe + token VASCO + PIN, Token mobilny Asseco MAA + PIN (mToken)

Wygląd formatek dla użytkownika

i) Autentykacja (logowanie) token VASCO:

Wybór metody autentykacji – Logowanie tokenem VASCO:



The screenshot shows a web form titled "Autoryzacja" (Authorization). The form has a dark green header bar with the title. Below the header, there is a light green background area. At the top of this area, there is a message: "Proszę wprowadzić Identyfikator użytkownika i Klucz w odpowiednie pola oraz nacisnąć przycisk 'Zatwierdź'." (Please enter the user ID and key in the appropriate fields and click the 'Zatwierdź' button). Below this message, there is a dropdown menu labeled "Logowanie:" with the selected option "Logowanie tokenem VASCO". Below the dropdown, there are two input fields: "Identyfikator użytkownika:" and "Klucz:". At the bottom of the form, there is a button labeled "Zatwierdź".

ii) Autoryzacja (podpisywanie) Tokenem mobilnym Asseco MAA:

Zlecenie do autoryzacji:



The screenshot shows a web form titled "Przelew - akceptowanie" (Payment - acceptance). The form has a dark blue header bar with the title. Below the header, there is a light blue background area. The form contains a table with the following data:

Referencje:	
Rachunek do obciążenia:	70 8818 0009 2001 0010 7695 0001 Podstawowy
Nazwa kontrahenta:	Kowalski Jan
Nr rachunku kontrahenta:	43 8818 0009 2001 0010 7695 0002
Tytułem:	sasasas
Przelew VAT:	Nie
Kwota:	199,00 PLN
Droga płatności:	Elixir
Data:	2019-08-27
Zleceniodawca:	Firma ETEST Bardzo testowa firma

Below the table, there are two buttons: "Podpisz" (Sign) and "Zamknij" (Close). At the bottom of the form, there is a log entry: "Log: 2019-08-27 12:05 Nowy przelew - Janusz Plicht".

Oczekiwanie na podpis tokenem mobilnym Asseco MAA:

Przelew - akceptowanie

Referencje:	
Rachunek do obciążenia:	70 8818 0009 2001 0010 7695 0001 Podstawowy
Nazwa kontrahenta:	Kowalski Jan
Nr rachunku kontrahenta:	43 8818 0009 2001 0010 7695 0002
Tytułem:	sasasas
Przelew VAT:	Nie
Kwota:	199,00 PLN
Droga płatności:	Elxir
Data:	2019-08-27
Zleceniodawca:	Firma ETEST Bardzo testowa firma

**Powiadomienie autoryzacyjne zostało wysłane na urządzenie.
Pozostań na stronie i potwierdź operację w aplikacji mobilnej.**



Oczekiwanie na podpis aplikacją mobilną

Zamknij

Log:
2019-08-27 12:05 Nowy przelew - Janusz Plicht

Akceptacja w tokenie mobilnym Asseco MAA kończy proces autoryzacji:

15:54 LTE

ASSECO

← AUTORYZACJA OPERACJI →

Realizacja przelewu

11.00 PLN

Osoba:
adrian zwykly

Zobowiązanie:
08 1010 1010 0088 2014 9640 0000

Nr rachunku:
31 1020 0003 3862 2573 0105 5179

Tytułem:
zwykly test przelewu

Typ operacji:
zwykly

Data realizacji:
27.08.2019

✖ ODRZUĆ✔ AKCEPTUJ

15:55 LTE

ASSECO


← AUTORYZACJA OPERACJI →

Podaj PIN


Wprowadź PIN

1	2	3
4	5	6
7	8	9
	0	⊗


✔ ZATWIERDŹ



Autoryzacja



Powiadomienia



Ustawienia

2.2 Opis szczegółowy - Hasło stałe + token VASCO + PIN, Karta mikroprocesorowa (aplikacja SCSA) + PIN

Wygląd formatek dla użytkownika

i) Autentykacja (logowanie) token VASCO:

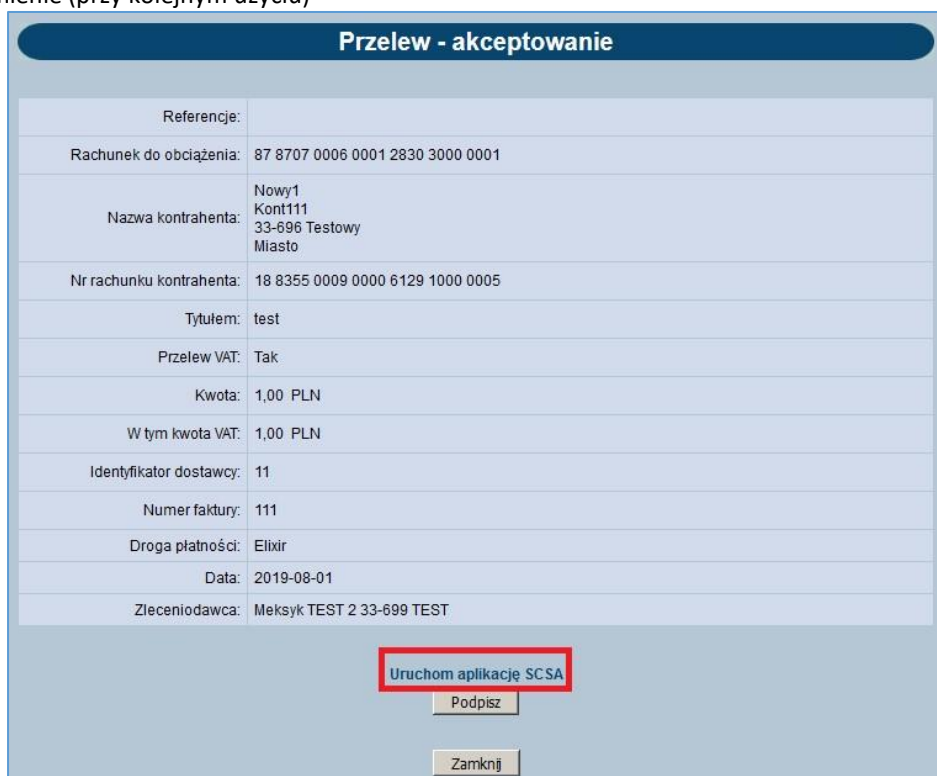
Wybór metody autentykacji – Logowanie tokenem VASCO:



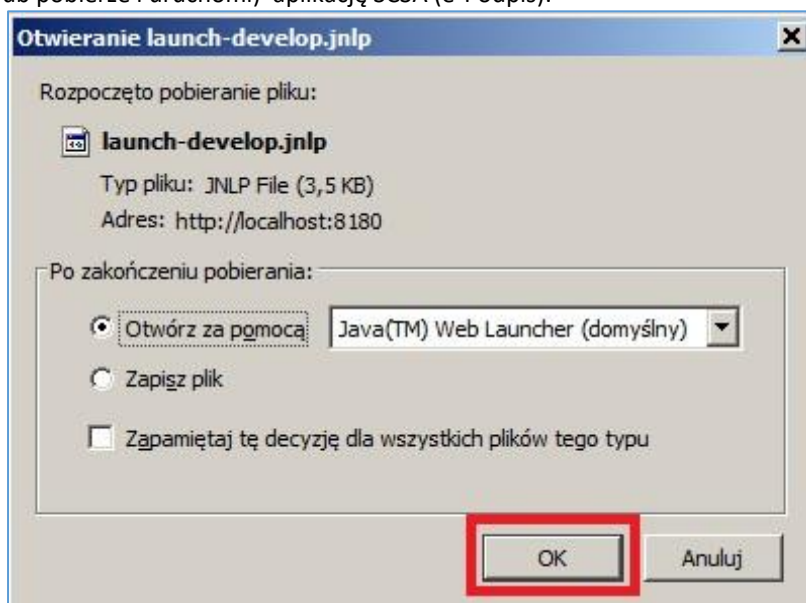
ii) autoryzacja (podpisywanie) kartą mikroprocesorową z aplikacją SCSA (e-Podpis):

Przed podpisem należy uruchomić link „Uruchom aplikację SCSA”. Spowoduje to:

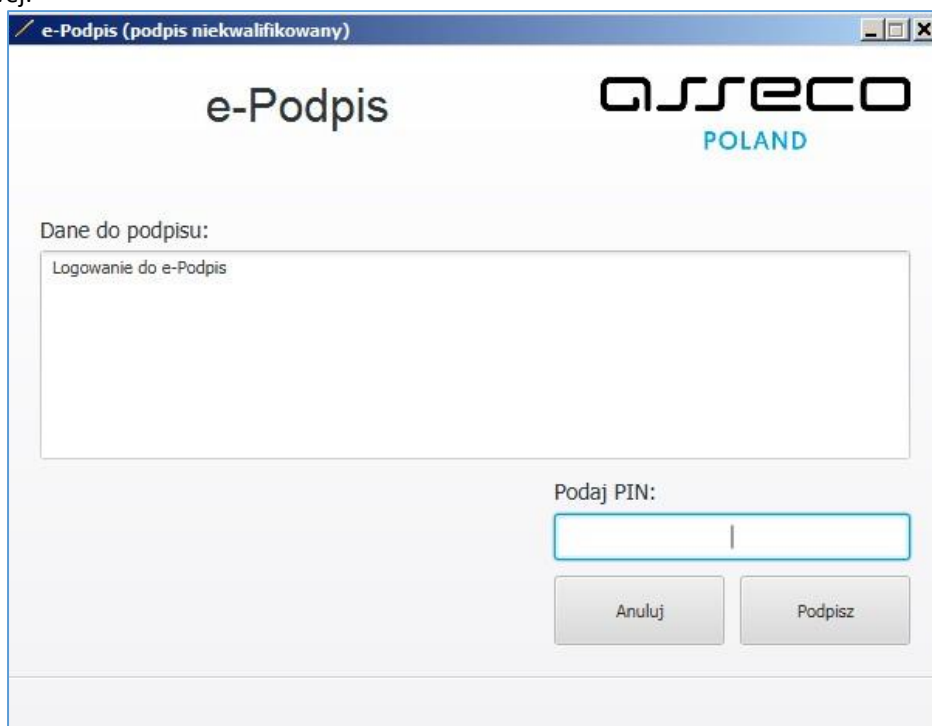
- pobranie (przy pierwszym użyciu dla nowej stacji roboczej), lub
- uruchomienie (przy kolejnym użyciu)



Uruchomienie linku „Uruchom aplikację SCSA” spowoduje, że przeglądarka automatycznie pobierze plik JNLP, który uruchomi (lub pobierze i uruchomi) aplikację SCSA (e-Podpis):



Po uruchomieniu pliku JNLP Użytkownikowi automatycznie pojawi się okno aplikacji SCSA (e-Podpis). Zalogowanie do aplikacji SCSA wymaga umieszczenia karty mikroprocesorowej w czytniku i wprowadzenia numeru PIN karty mikroprocesorowej:



Po uruchomieniu aplikacji SCSA (e-Podpis) i po podaniu PINu (dla logowania do e-Podpis), wybieramy przycisk [Podpisz]:

Przelew - akceptowanie	
Referencje:	
Rachunek do obciążenia:	87 8707 0006 0001 2830 3000 0001
Nazwa kontrahenta:	Nowy1 Kont111 33-696 Testowy Miasto
Nr rachunku kontrahenta:	18 8355 0009 0000 6129 1000 0005
Tytułem:	test
Przelew VAT:	Tak
Kwota:	1,00 PLN
W tym kwota VAT:	1,00 PLN
Identyfikator dostawcy:	11
Numer faktury:	111
Droga płatności:	Elixir
Data:	2019-08-01
Zleceniodawca:	Meksyk TEST 2 33-699 TEST
Uruchom aplikację SCSA	
<input type="button" value="Podpisz"/>	
<input type="button" value="Zamknij"/>	

użyciu przycisku [Podpisz] formatka „Przelew – akceptowanie” przejdzie w tryb „Oczekiwanie na podpis aplikacją SCSA”:

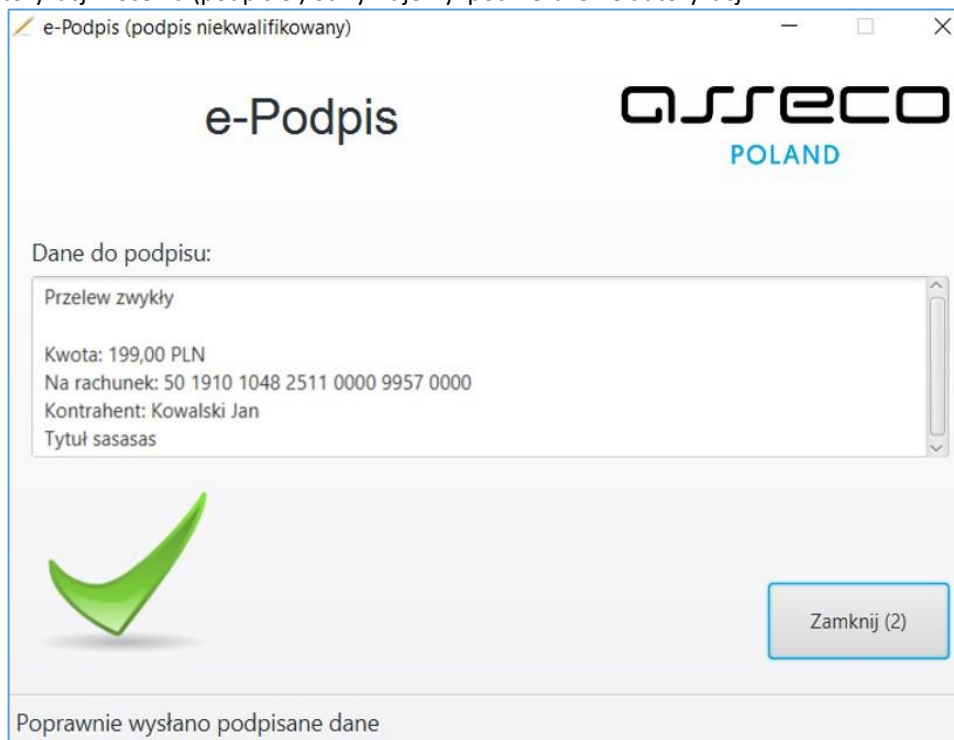
Przelew - akceptowanie	
Referencje:	
Rachunek do obciążenia:	87 8707 0006 0001 2830 3000 0001
Nazwa kontrahenta:	Nowy1 Kont111 33-696 Testowy Miasto
Nr rachunku kontrahenta:	18 8355 0009 0000 6129 1000 0005
Tytułem:	test
Przelew VAT:	Tak
Kwota:	1,00 PLN
W tym kwota VAT:	1,00 PLN
Identyfikator dostawcy:	11
Numer faktury:	111
Droga płatności:	Elixir
Data:	2019-08-01
Zleceniodawca:	Meksyk TEST 2 33-699 TEST
<p>Powiadomienie autoryzacyjne zostało wysłane na aplikację SCSA. Pozostań na stronie i potwierdź operację w aplikacji SCSA.</p>  <p>Oczekiwanie na podpis aplikacją SCSA</p>	
<input type="button" value="Zamknij"/>	

Następnie należy wykonać autoryzację zlecenia (podpis) w aplikacji SCSA. W tym celu wymagane jest umieszczenie karty mikroprocesorowej w czytniku (lub bezpośrednio w porcie USB – wersja mini kart mikroprocesorowych) i wprowadzenie numeru PIN karty mikroprocesorowej:



The screenshot shows a window titled "e-Podpis (podpis niekwalifikowany)" with the "e-Podpis" logo and "ASSECO POLAND" branding. Under "Dane do podpisu:", a scrollable box contains the following text: "Przelew zwykły", "Kwota: 199,00 PLN", "Na rachunek: 50 1910 1048 2511 0000 9957 0000", "Kontrahent: Kowalski Jan", and "Tytuł sasasas". To the right, there is a "Podaj PIN:" label above a text input field containing four dots. Below the input field are two buttons: "Anuluj" and "Podpisz".

poprawnej autoryzacji zlecenia (podpisie) otrzymujemy potwierdzenie autoryzacji:



The screenshot shows the same "e-Podpis" window, but now with a large green checkmark icon on the left. The "Dane do podpisu:" section remains the same. A "Zamknij (2)" button is now visible in the bottom right corner. At the bottom of the window, a status bar displays the message "Poprawnie wysłano podpisane dane".

3. Pytania i odpowiedzi

3.1. Jakie są wymagania aplikacji SCSA?

Aplikacja SCSA pracuje na urządzeniach klasy PC na systemach operacyjnych Windows 7 i nowszych. Dla poprawnego działania aplikacji SCSA wymagane jest zainstalowanie darmowej wersji JAVA Open JDK.

3.2. Skąd pobrać instalator dla javy Open JDK?

Instalator Open JDK zostanie umieszczony na stronie <https://bsszczytno.pl/bankowosc-internetowa>.