



BANK SPÓŁDZIELCZY W GORLICACH

ul. Stróżowska 1

REGULAMIN KORZYSTANIA Z FUNKCJI DWUETAPOWEGO LOGOWANIA KLUCZAMI U2F

Postanowienia ogólne.

§1.

1. „Regulamin korzystania z funkcji dwuetapowego logowania kluczami **U2F**” zwany dalej Regulaminem obowiązuje w Banku Spółdzielczym w Gorlicach z siedzibą w Gorlicach ul. Stróżowska 1, 38-300 Gorlice, e-mail: biuro@bs.gorlice.pl, www.bs.gorlice.pl, którego akta rejestrowe przechowywane są w Sądzie Rejonowym dla Krakowa Śródmieścia w Krakowie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, wpisanym do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem 00001376595, NIP 738 00 09 085.
2. Regulamin określa zasady korzystania z kluczy U2F w celu dwuetapowego logowania do bankowości elektronicznej.
3. Klucze U2F są nową funkcjonalnością zabezpieczeń bankowości elektronicznej chroniący Użytkownika przed phishingiem i wyciekami danych do logowania.
4. Nowe metody zabezpieczeń są udostępnione wszystkim posiadaczom bankowości elektronicznej Banku. Warunkiem skorzystania jest dodanie w ustawieniach bankowości nowej metody logowania za pomocą kluczy U2F.
5. Zakup klucza odbywa się przez Użytkownika bezpośrednio od Producenta bez udziału Banku eliminując marżę i wprowadzając dowolność w wyborze sprzętowej klucza według preferencji Użytkownika (klucz standardowy, biometryczny, etc).
6. Bank zaleca zakup urządzeń typu: Security Key NFC by Yubico (USB-A lub USB-C)
7. Nowa metoda zabezpieczeń kluczami U2F nie jest obligatoryjna dla Użytkowników bankowości elektronicznej, ale zalecana do stosowania.

§2.

Użyte w Regulaminie określenia oznaczają:

- 1) autoryzacja - wyrażenie przez Posiadacza rachunku lub osobę przez niego upoważnioną do dysponowania środkami na rachunku zgody na wykonanie transakcji płatniczej lub innej dyspozycji w formie przewidzianej niniejszym Regulaminem

- 2) Bank – Bank Spółdzielczy w Gorlicach z siedzibą w Gorlicach ul. Stróżowska 1;
- 3) forma maskowana – oznacza odpowiednie zabezpieczenia informacji w niej zawartych; w przypadku hasła aktywacyjnego forma maskowana oznacza pokrycie hasła odpowiednim materiałem, którego usunięcie umożliwi jego odczytanie;
- 4) Indywidualne dane uwierzytelniające – indywidualne dane zapewniane Posiadaczowi rachunku /Użytkownikowi karty przez bank do celów uwierzytelniania;
- 5) 5) Kod identyfikacyjny:
 - a) kod PIN (Personal Identification Number) stanowiący poufny numer lub inne oznaczenie, które łącznie z danymi zawartymi na Karcie stanowią unikatowy identyfikator służący do elektronicznej identyfikacji Posiadacza rachunku/Użytkownika karty, przypisany do danej Karty i znany tylko Posiadaczowi rachunku/ Użytkownikowi karty
 - b) e-PIN - kod stanowiący poufny numer służący do silnego uwierzytelnienia Użytkownika w aplikacji mobilnej, ustanawiany samodzielnie przez Użytkownika
 - c) kod uwierzytelnienia – kod wykorzystywany w procesie silnego uwierzytelnienia w systemie bankowości elektronicznej, ustanawiany samodzielnie przez Użytkownika w systemie bankowości elektronicznej lub ustanawiany samodzielnie przez Użytkownika karty w portalu kartowym dla płatności karta w Internecie,
 - d) kod QR – Quick Response Code zakodowana informacja tekstowa w postaci kwadratu i z wzorem graficznym, najczęściej w kolorze białym i czarnym;
 - e) kod SMS - metoda autoryzacji w bankowości elektronicznej oparta na silnym uwierzytelnieniu zgodnym z PSD2 i oparta na kodzie jednorazowym, kontekstowo powiązany z wykonywaną transakcją płatniczą służący do autoryzacji dyspozycji i transakcji płatniczych składanych w usłudze bankowości elektronicznej oraz transakcji kartą w Internecie;
- 6) Posiadacz rachunku – osoba fizyczna, która zawarła z Bankiem Umowę, przy czym w przypadku rachunku wspólnego przez Posiadacza rachunku należy rozumieć każdego ze Współposiadaczy;
- 7) rachunek bankowy/ rachunek płatniczy – rachunek służący do wykonywania transakcji płatniczych oferowany i prowadzony przez Bank dla osób fizycznych;
- 8) silne uwierzytelnienie (SCA) - uwierzytelnianie zapewniające ochronę poufności danych w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii:
 - a) wiedza o czymś, o czym wie wyłącznie Użytkownik/ Użytkownik karty,
 - b) posiadanie czegoś, co posiada wyłącznie Użytkownik/Użytkownik karty,
 - c) cechy charakterystyczne Użytkownika/ Użytkownika karty,będących integralną częścią tego uwierzytelniania oraz niezależnych w taki sposób, że naruszenie jednego z tych elementów nie osłabia wiarygodności pozostałych;
- 9) strona internetowa Banku – www.bs.gorlice.pl, strona na której dostępne są min. aktualne wersje Tabeli oprocentowania, Tabeli opłat i prowizji oraz Tabeli kursowej oraz instrukcja korzystania z kluczy U2F;

- 10) system bankowości elektronicznej – system umożliwiający samoobsługowy dostęp do rachunków bankowych Posiadacza rachunku oraz dostęp do innych produktów bankowych za pomocą sieci Internet i przeglądarki internetowej, oraz system obsługi telefonicznej oferowany w ramach usługi bankowości elektronicznej;
- 11) system bankowości mobilnej - system umożliwiający samoobsługowy dostęp do rachunków bankowych Posiadacza rachunku oraz dostęp do innych produktów bankowych za pomocą sieci Internet i za pomocą aplikacji zainstalowanej na urządzeniu mobilnym działającym w sieci bezprzewodowej, oferowany w ramach usługi bankowości elektronicznej;
- 12) unikatowy identyfikator- kombinacja liter, liczb lub symboli określona przez Bank i przekazana Posiadaczowi rachunku w celu jednoznacznej identyfikacji Posiadacza rachunku lub jego rachunku bankowego;
- 13) usługa bankowości elektronicznej - usługa polegająca na dostępie do rachunku płatniczego przez Internet, umożliwiająca sprawdzenie salda rachunku płatniczego, zmianę limitów dla płatności bezgotówkowych i transakcji dokonywanych przy użyciu karty debetowej lub złożenie innego rodzaju dyspozycji do rachunku;
- 14) Ustawa o usługach płatniczych – Ustawa z dnia 19 sierpnia 2011r. o usługach płatniczych;
- 15) Uwierzytelnienie - procedura umożliwiająca Bankowi weryfikację tożsamości Posiadacza rachunku/Użytkownika/Użytkownika karty lub ważności stosowania danego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających;
- 16) Użytkownik – Posiadacz rachunku lub osoba fizyczna posiadająca pełną zdolność do czynności prawnych, która jest uprawniona do dysponowania rachunkiem w systemie bankowości elektronicznej w imieniu i na rzecz Posiadacza rachunku;
- 17) klucz sprzętowy - urządzenie zgodne ze standardem U2F, podłączane do komputera lub urządzenia mobilnego (lub poprzez interfejs NFC w przypadku urządzeń wspierających NFC), używany w procesie uwierzytelniania lub autoryzacji w systemie bankowości elektronicznej.

§3.

W ramach niniejszego Regulaminu, Bank określa zasady korzystania z kluczy sprzętowych:

- 1) Klucz sprzętowy aktywny jest po dodaniu go w bankowości elektronicznej przez klienta. Posiadacz rachunku może dodać kilka kluczy do jednego użytkownika,
- 2) Klucz sprzętowy służy jako alternatywne (do sms lub systemu bankowości mobilnej) zabezpieczenie logowania do bankowości elektronicznej. Oprócz identyfikatora i hasła po aktywacji klucza sprzętowego będzie on wymagany w procesie logowania jako dodatkowy element zabezpieczenia.
- 3) Posiadacz rachunku w dowolnym czasie może zmienić metodę logowaniu dwuetapowego na inną akceptowaną przez bank metodę autoryzacji (np. sms, system bankowości mobilnej)
- 4) Użytkownik ma obowiązek zabezpieczać klucze sprzętowe przed osobami trzecimi tak jak o każde inne urządzenie/środek płatniczy zgodnie z tym jak opisano to w regulaminie o prowadzenie rachunku. Nie należy udostępniać klucza sprzętowego osobom trzecim a w przypadku zgubienia należy niezwłocznie zgłosić fakt bankowi i usunąć zgubiony klucz z bankowości elektronicznej.
Użytkownicy zobowiązują się do przechowywania i skutecznej ochrony kluczy sprzętowych z zachowaniem należytej staranności – w tym także do należytej ochrony komputerów, z których korzystają w systemie bankowości elektronicznej. Użytkownicy zobowiązani są do

nieprzechowywania różnych środków dostępu razem w jednym miejscu oraz są zobowiązani do niezwłocznego zgłaszania Bankowi utraty lub zniszczenia środków dostępu lub udostępnieniu środków dostępu osobom nieuprawnionym.

- 5) Bank nie gwarantuje działania wszystkich typów kluczy sprzętowych U2F.
- 6) Klucz sprzętowy nie jest wymagany do logowania w systemie bankowości mobilnej.

2023-09-25