NICOLAUS BANK

Regulamin użytkowania klucza zabezpieczeń U2F

w Nicolaus Banku Spółdzielczym w Toruniu

Toruń, październik 2023

Rozdział 1. Postanowienia ogólne

§ 1

1. Niniejszy „Regulamin użytkowania klucza zabezpieczeń U2F w Nicolaus Banku Spółdzielczym w Toruniu" , zwany dalej regulaminem, określa zasady użytkowania klucza bezpieczeństwa dla dwuetapowego logowania do bankowości internetowej.
2. Klucz U2F jest nową funkcjonalnością zabezpieczająca bankowość internetową klienta.
3. Wymagania techniczne dla stosowanego klucza oraz przeglądarki zawarte są w załączniku. Rekomendowany klucz bezpieczeństwa: **YubiKey 5 Series**.
4. Nowa metoda zabezpieczeń kluczem U2F nie jest obligatoryjna dla Użytkowników bankowości elektronicznej, ale zalecana do stosowania.

§ 2

Użyte w regulaminie określenia oznaczają:

1) **klucz zabezpieczeń** - urządzenie zewnętrzne, podłączane do komputera lub urządzenia mobilnego, używane w procesie logowania i uwierzytelniania wieloskładnikowego w Systemie bankowości internetowej.
2) **lista kluczy zabezpieczeń** – lista widoczna w Systemie bankowości internetowej zawierająca wszystkie klucze, które użytkownik uznaje za bezpieczne, które spełniają wymogi techniczne odpowiednie dla tego typu urządzeń. Użytkownik może modyfikować listę aktywowanych kluczy przez dodawanie lub usuwanie z niej poszczególnych kluczy. Lista może zawierać jeden lub więcej kluczy;
3) **środki dostępu do Systemu Bankowości Internetowej** – identyfikator Użytkownika, hasło aktywacyjne, hasło użytkownika dostarczane w postaci wydruku lub w formie elektronicznej, hasła jednorazowe dostarczane w formie elektronicznej, klucze zabezpieczeń - umożliwiające uwierzytelnianie użytkownika i autoryzacje transakcji płatniczych i innych dyspozycji w Systemie bankowości internetowej.

Rozdział 2 Uwierzytelnienie użytkownika

§ 3

1. Uwierzytelnienie użytkownika jest wymagane zarówno podczas logowania się do Systemu, jak i podczas inicjowania elektronicznej dyspozycji płatniczej. Uwierzytelnianie użytkownika podczas logowania do Systemu bankowości internetowej obejmuje następujące czynności:
   1) podanie poprawnego loginu,
   2) podanie hasła,
   3) a w przypadku, gdy jest to wymagane prawem lub wynika ze względów bezpieczeństwa dodatkowo także – podanie odpowiedniego kodu autoryzacyjnego lub potwierdzenia w aplikacji mobilnej, gdy klient

posiada aplikację mobilną lub **użycia klucza zabezpieczeń**, gdy klient posiada aktywny klucz na liście kluczy zabezpieczeń.

2. Jeżeli podczas logowania się użytkownika do Systemu, Bank wymaga podania wszystkich informacji, o których mowa w pkt 1) - 3) nazywa się to silnym uwierzytelnianiem. Bank stosuje silne uwierzytelnianie, gdy jest to wymagane przepisami prawa.
3. Uwierzytelnienie użytkownika za pomocą klucza wymaga od użytkownika rejestracji klucza U2F w systemie bankowości internetowej oraz wyrażenia zgody na dodatkową metodę uwierzytelnienia.
4. W bankowości internetowej użytkownik widzi listę aktywowanych kluczy zabezpieczeń, którą może modyfikować przez dodawanie lub usuwanie z niej poszczególnych kluczy.

Rozdział 3. Zasady bezpieczeństwa

§ 4

1. Użytkownik ma obowiązek zabezpieczać klucze sprzętowe przed osobami trzecimi tak jak każde inne urządzenie/środek płatniczy zgodnie z tym jak opisano to w regulaminie o prowadzenie rachunku.
2. Nie należy udostępniać klucza sprzętowego osobom trzecim a w przypadku zgubienia należy niezwłocznie zgłosić fakt bankowi i usunąć zgubiony klucz z bankowości elektronicznej.
3. 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.
4. 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. Użytkownik zobowiązany jest do złożenia dyspozycji zablokowania Systemu, w sytuacji powzięcia informacji o powstaniu zagrożenia bezpiecznego przechowywania przez użytkownika klucza zabezpieczeń znajdującego się na liście kluczy zabezpieczeń.

Załącznik

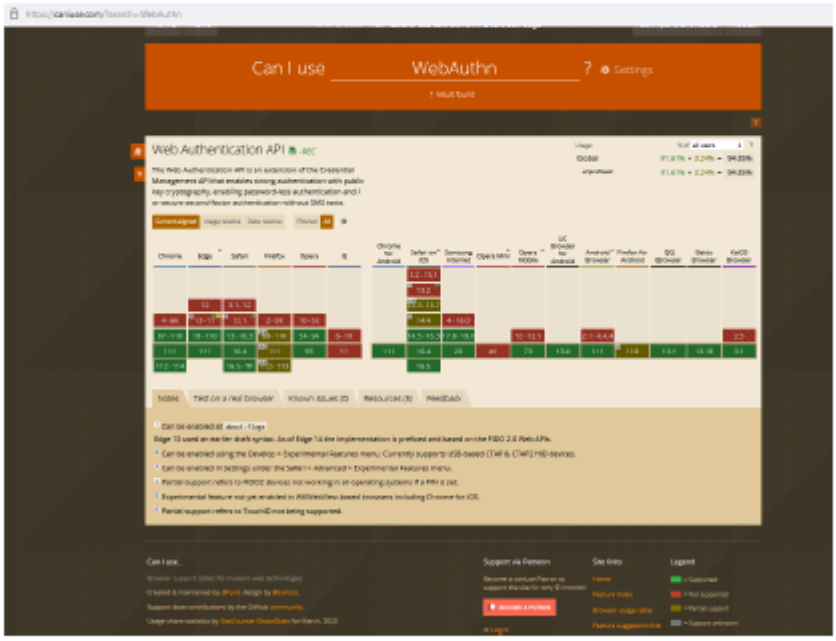
WYMOGI TECHNICZNE KLUCZY ZABEZPIECZEŃ

1. Przeglądarka
Wymagana obsługa Webauthn
Przeglądarki wspierające WebAuthn: https://caniuse.com/?search=WebAuthn

Chrome – od wersji 67
Edge – od wersji 18
Safari – od wersji 13
Firefox – od wersji 60(*)
Opera – od wersji 54

Chrome for Android – od wersji 111
Safari on iOS – od wersji 13.3(*), zalecana wersja minimalna: 14.5
Samsung Internet – od wersji 17
Opera Mobile – od wersji 73
Firefox for Android – od wersji 110(*)

(*) Częściowe wsparcie odnosi się do urządzeń FIDO2, które nie działają we wszystkich systemach operacyjnych, jeśli ustawiony jest kod PIN.



2. Klucz
Wymagana obsługa FIDO2 (CTAP2) lub FIDO U2F (CTAP1)
Rekomendowane klucze bezpieczeństwa: **YubiKey 5 Series**

Zmiany powodujące rozszerzenie zakresu urządzeń spełniających wymogi techniczne kluczy zabezpieczeń nie stanowią zmiany warunków umownych.