Bank Spółdzielczy w Siedlcu

Regulamin korzystania z funkcji dwuetapowego logowania kluczami U2F

Postanowienia ogólne

§ 1

1. Niniejszy „Regulamin korzystania z funkcji dwuetapowego logowania kluczami U2F" zwany dalej Regulaminem określa zasady korzystania z kluczy U2F w celu dwuetapowego logowania do bankowości elektronicznej.
2. Klucze U2F są nową funkcjonalnością zabezpieczeń bankowości elektronicznej chroniąc Użytkownika przed phishingiem i wyłudzeniami danych do logowania.
3. Nowe metody zabezpieczeń są udostępnione wszystkim posiadaczom bankowości elektronicznej Banku. Warunkiem skorzystania jest dodanie w ustawieniach bankowości nowej metody logowania za pomocą kluczy U2F.
4. Zakup klucza odbywa się przez Użytkownika w placówce Banku. Bank oferuje klucze YubiKey 5 NFC /USB-A/.
5. Klucz U2F jest udostępniony bezzwrotnie przez Bank za pobraniem prowizji zgodnie z Tabelą opłat i prowizji.
6. Nowa metoda zabezpieczeń kluczami U2F nie jest obligatoryjna dla Użytkowników bankowości elektronicznej, ale zalecana do stosowania.

§ 2

Użyte w Regulaminie określenia oznaczają:

1/ **autoryzacja** - udzielenie przez użytkownika zgody na wykonanie dyspozycji, w tym zlecenia płatniczego, przed jej realizacją przez Bank, w sposób określony w Umowie lub niniejszym regulaminie, poprzedzone uwierzytelnieniem lub silnym uwierzytelnieniem użytkownika;

2/ **Bank** –Bank Spółdzielczy w Siedlcu;

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/ 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 powiązanym 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, w przypadku rachunku wspólnego każdy 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.banksiedlec.pl;

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;

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 zabezpieczeń** - klucz zabezpieczeń - urządzenie zewnętrzne, podłączane do komputera lub urządzenia mobilnego, używane w procesie logowania i uwierzytelniania wieloskładnikowego w systemie bankowości internetowej. Wymogi techniczne urządzeń możliwych do użycia przez użytkownika zawiera **zał. nr 2.**

§ 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 (sposób dodania klucza do bankowości elektronicznej opisany został w **zał. nr 1**).
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 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

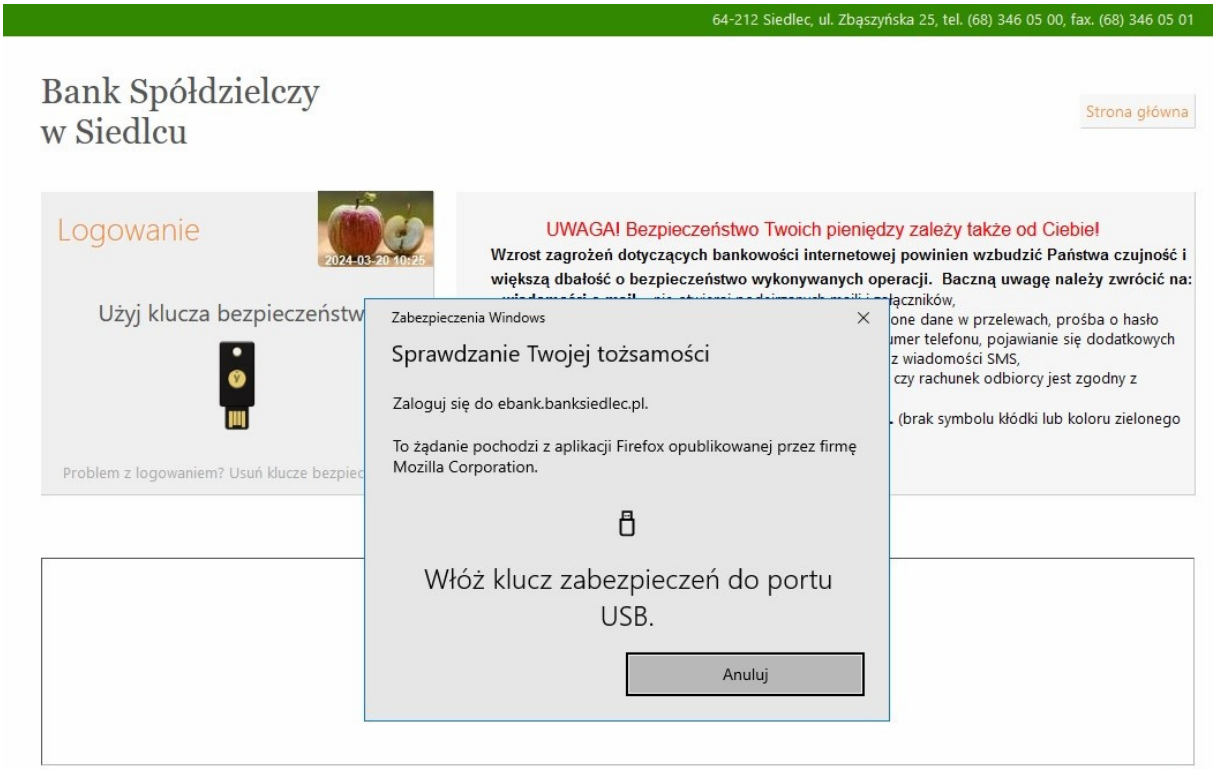
elektronicznej. Użytkownicy zobowiązani są do nieprzechowywania różnych środków dostępu razem w jednym miejscu oraz są zobowiązani do niezwłocznego zgłaszania Bankowi utraty lub zniszczenia środków dostępu lub udostępnieniu środków dostępu osobom nieuprawnionym.

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

Załącznik nr 1

1. Logowanie z użyciem klucza bezpieczeństwa U2F

Logowanie do bankowości elektronicznej jest dwuetapowe:
- należy wpisać identyfikator i hasło,
- należy użyć klucza bezpieczeństwa i potwierdzić logowanie:

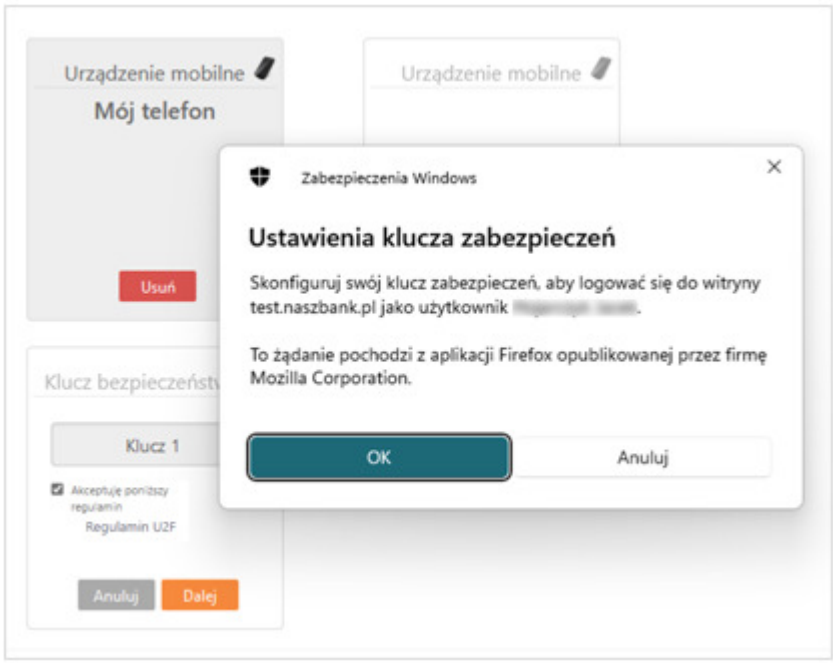


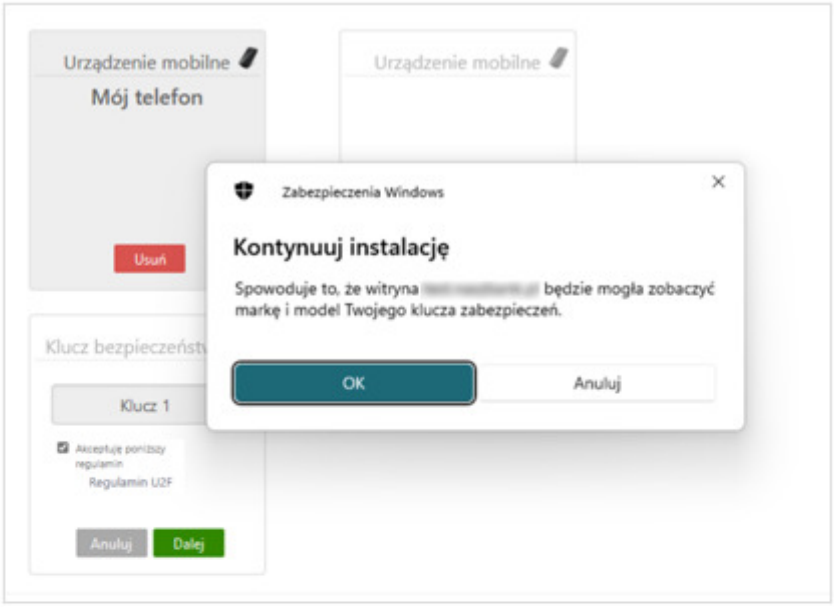
Dodanie klucza bezpieczeństwa opisane jest w rozdziale: Dodanie klucza bezpieczeństwa.

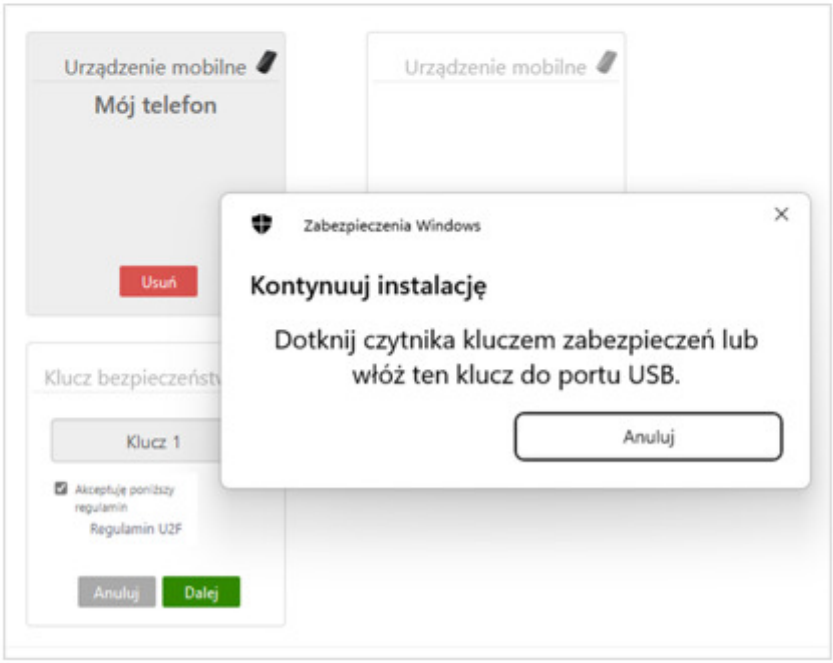
2. Dodanie klucza bezpieczeństwa w IB

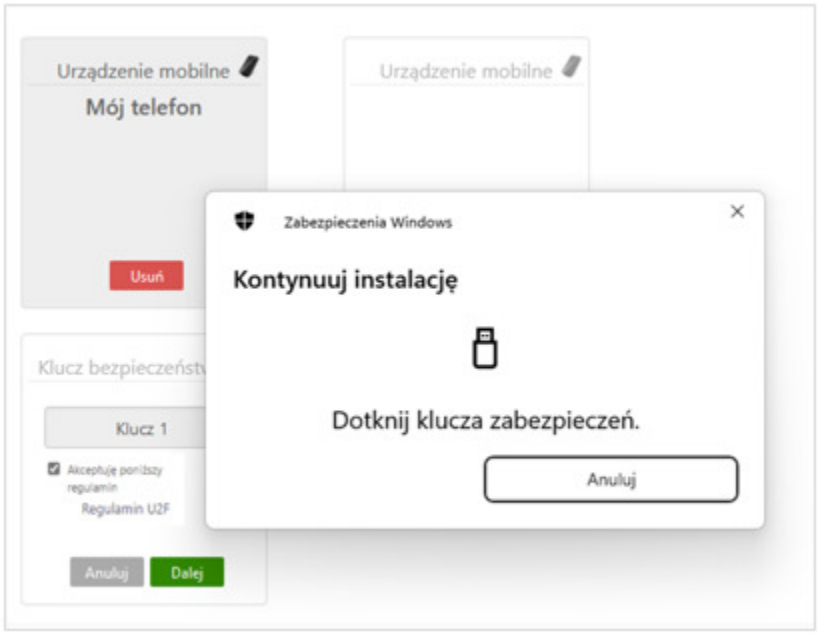
W Internet Banking za pomocą opcji **Kanały dostępu i urządzenia**
W Internet Banking Firm za pomocą opcji **Kanały i Klucze bezpieczeństwa**

Należy wybrać *Klucz bezpieczeństwa* → **Dodaj** i postępować zgodnie z komunikatami wyświetlonymi w systemie. Klucz bezpieczeństwa służy do logowania do bankowości elektronicznej.


Urządzenie mobilne
Mój telefon
Usuń
Urządzenie mobilne
Klucz bezpieczeństw
Klucz 1
Akceptuję poniższy regulamin
Regulamin U2F
Anuluj
Dalej
Zabezpieczenia Windows
Ustawienia klucza zabezpieczeń
Skonfiguruj swój klucz zabezpieczeń, aby logować się do witryny test.naszbank.pl jako użytkownik
To żądanie pochodzi z aplikacji Firefox opublikowanej przez firmę Mozilla Corporation.
OK
Anuluj


Urządzenie mobilne
Mój telefon
Urządzenie mobilne
Usuń
Zabezpieczenia Windows
Kontynuuj instalację
Spowoduje to, że witryna będzie mogła zobaczyć markę i model Twojego klucza zabezpieczeń.
OK
Anuluj
Klucz bezpieczeństw
Klucz 1
Akceptuję poniższy regulamin
Regulamin U2F
Anuluj
Dalej


Urządzenie mobilne
Mój telefon
Urządzenie mobilne
Usuń
Zabezpieczenia Windows
Kontynuuj instalację
Dotknij czytnika kluczem zabezpieczeń lub włóż ten klucz do portu USB.
Anuluj
Klucz bezpieczeństw
Klucz 1
Akceptuję poniższy regulamin
Regulamin U2F
Anuluj
Dalej


Urządzenie mobilne
Mój telefon
Usuń
Urządzenie mobilne
Klucz 1
Akceptuję poniższy regulamin
Regulamin U2F
Anuluj
Dalej
Zabezpieczenia Windows
Kontynuuj instalację
Dotknij klucza zabezpieczeń.
Anuluj

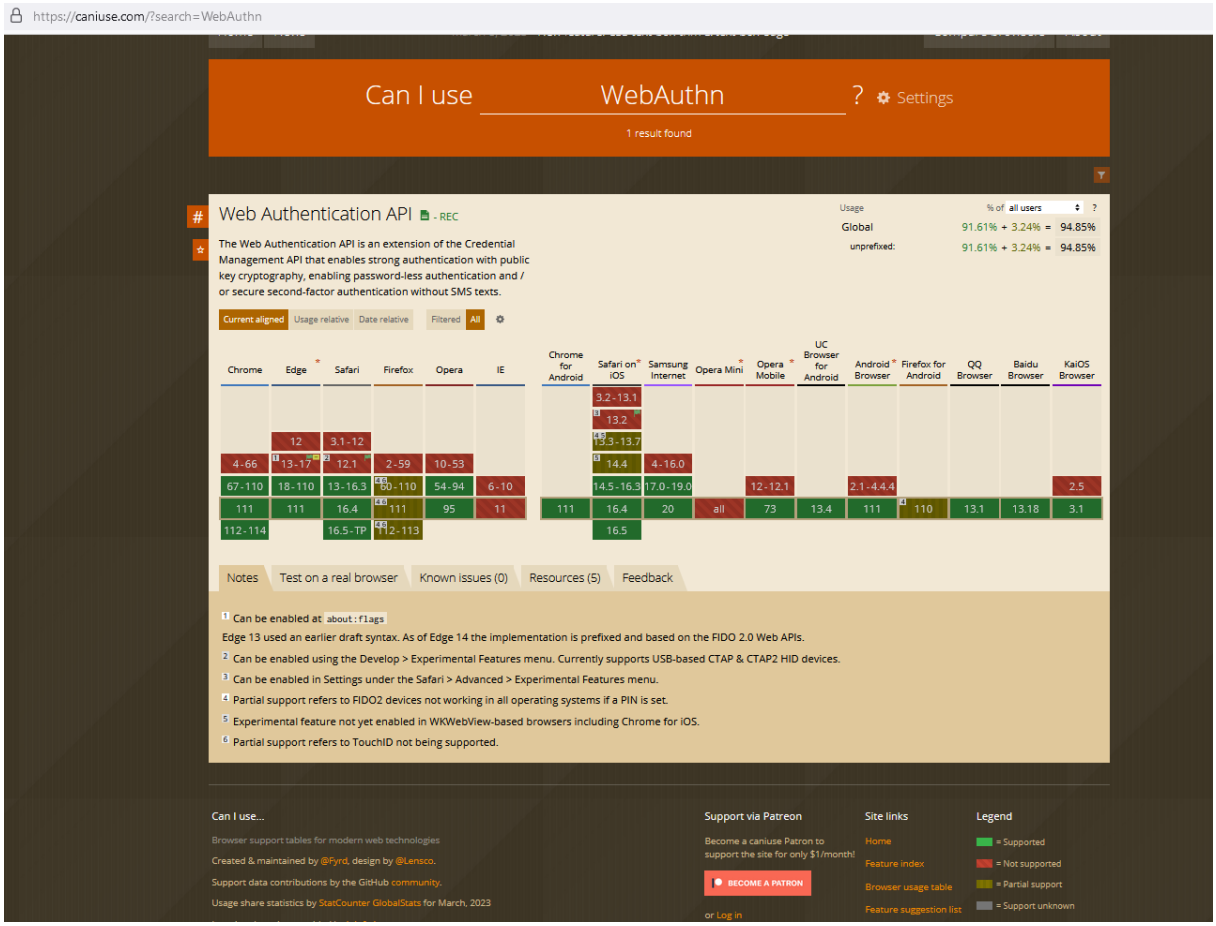
WYMOGI TECHNICZNE KLUCZY ZABEZPIECZEŃ

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.