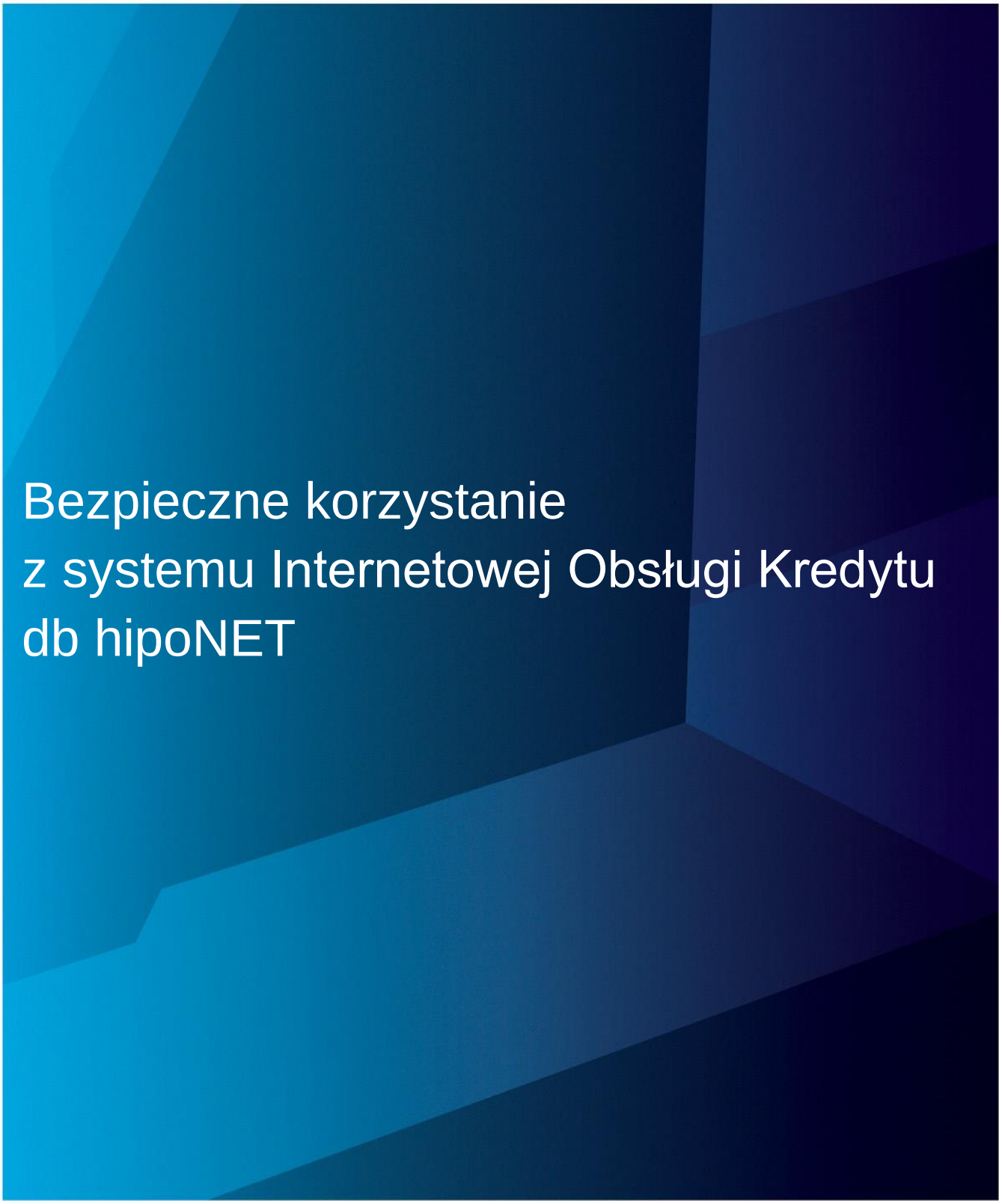
Deutsche Bank



Bezpieczne korzystanie z systemu Internetowej Obsługi Kredytu db hipoNET

Spis treści

Wstęp 3
Ogólne Zasady bezpieczeństwa 3
Bezpieczny komputer, tablet, smartfon 3
Konfiguracja przeglądarki 4
Bezpieczne Logowanie 5
Zabezpieczenia zastosowane w systemie db hipoNET 8
Numer Identyfikacyjny Klienta (NIK) i Kod Dostępu 8
Sytuacje alarmowe 9

Wstęp

Deutsche Bank Polska S.A. ogromną uwagę poświęca Twojemu bezpieczeństwu.

Dlatego też dostęp do Internetowej Obsługi Kredytu chroniony jest z wykorzystaniem najnowocześniejszych i bardzo skutecznych metod zabezpieczeń.

Twoje bezpieczeństwo w internecie zależy również od Ciebie. Dlatego prosimy zapoznaj się ze wskazówkami, które pomogą w bezpiecznym korzystaniu z naszego serwisu.

Niniejszy podręcznik ma na celu przybliżenie Ci podstawowych zasad bezpieczeństwa oraz wskazanie stanu zabezpieczeń, który pozwoli lepiej chronić Twój komputer, tablet oraz smartfon przed ewentualnymi próbami przechwycenia poufnych danych.

Ogólne Zasady bezpieczeństwa

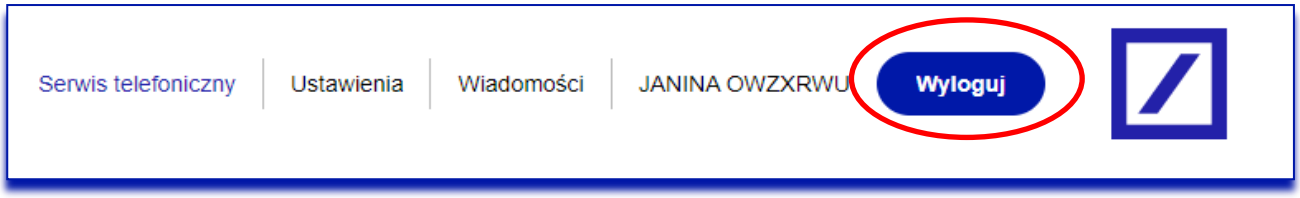
Bezpieczne korzystanie z systemu db hipoNET zależy w znacznym stopniu od Ciebie!

Bezpieczny komputer, tablet, smartfon

Dbaj o bezpieczeństwo swojego urządzenia!

Jedną z najważniejszych czynności, poprzedzających korzystanie z systemu Internetowej Obsługi Kredytu db hipoNET, jest właściwe przygotowanie urządzenia oraz zainstalowanego w nim oprogramowania. Poniżej znajdziesz szczegółowe informacje jak zabezpieczyć swój komputer, tablet oraz smartfon.

1. Do korzystania z Internetowej Obsługi Kredytów db hipoNET używaj legalnego systemu operacyjnego, dla którego producent regularnie dostarcza aktualizacje.
2. Instaluj tylko legalne oprogramowanie, nie instaluj oprogramowania pochodzącego z nieznanych źródeł.
3. Zabezpiecz swój komputer, tablet oraz smartfon programem antywirusowym oraz antyspamowym.
4. Używaj osobistego Firewalla – pozwoli on Tobie lepiej chronić się przed ingerencją z zewnątrz i ograniczy dostęp do informacji o zasobach Twojego urządzenia.
5. Pamiętaj o regularnych aktualizacjach systemu operacyjnego oraz zainstalowanego na nim oprogramowania, w tym w szczególności oprogramowania antywirusowego (wraz z bazą sygnatur wirusów).
6. Pamiętaj o cyklicznym skanowaniu antywirusowym całego systemu zgodnie z zaleceniami producenta oprogramowania antywirusowego. Chroń swój system pocztowy przed przychodzącym spamem. Pamiętaj, że wiadomości e-mail to jedna z najpopularniejszych dróg, jaką mogą do Ciebie trafić wirusy i informacje, których celem jest wyłudzenie poufnych danych (takich jak NIK czy Kod Dostępu).
7. Nie otwieraj załączników do wiadomości, których nie oczekiwałeś (ani samych wiadomości, których tytuł czy nadawca wzbudzają podejrzenie próby dokonania oszustwa).
8. Pamiętaj, że Bank nie wysyła wiadomości e-mail, w których prosi o zainstalowanie dodatkowego oprogramowania (aktualizację lub podanie poufnych danych).
9. Korzystaj z systemu Internetowej Obsługi Kredytu tylko na zaufanych urządzeniach. Nie jest zalecane logowanie się do systemu db hipoNET z urządzeń ogólnodostępnych (np. w kawiarenkach internetowych) oraz poprzez publiczne sieci WiFi (w tzw. hot-spotach).
10. Twoja przeglądarka internetowa powinna mieć wprowadzone zalecane przez Bank ustawienia (patrz. „Konfiguracja przeglądarki").
11. Nigdy nie pozostawiaj urządzenia bez nadzoru w czasie, kiedy zalogowany jesteś do systemu Internetowej Obsługi Kredytów.
12. Po zakończeniu pracy z db hipoNET pamiętaj o wylogowaniu się z systemu. W celu wylogowania z db hipoNET korzystaj z opcji „Wyloguj". Nie zamykaj systemu poprzez zamknięcie karty bądź okna przeglądarki internetowej.



Konfiguracja przeglądarki

Zabezpiecz swoją przeglądarkę!

1. Korzystaj z najnowszych wersji przeglądarek internetowych.

   Rekomendujemy aktualizację przeglądarki internetowej do najnowszej wersji dostępnej na rynku.

Przeglądarki internetowe dedykowane dla systemu db hipoNET		
Nazwa oraz wersja przeglądarki internetowej	db hipoNET [1]	
	urządzenie mobilne	Komputer PC / laptop
Microsoft EDGE od wersji 15.x	n/d	+
Mozilla Firefox od wersji 47.x	n/d	+
Google Chrome od wersji 69.x	n/d	+
Google Chrome Mobile od wersji 69.x	+	n/d
Apple Safari od wersji 9.x	n/d	+
Apple Safari Mobile od wersji 9.x	+	n/d

[1] Dostępny pod adresem: https://dbhiponet.deutschebank.pl

   Informację o wersji posiadanej przeglądarki oraz protokole szyfrowania znajdziesz wybierając z menu opcję „Pomoc", a następnie w zależności od przeglądarki:
   - Microsoft Edge → Ustawienia → Pomoc i opinia → Internet Edge – informacje
   - Google Chrome → Ustawienia Google Chrome → Google Chrome – informacje
   - Mozilla Firefox → O Mozilli Firefox
   - Apple Safari → Safari

2. Przed logowaniem sprawdź, czy Twoja przeglądarka obsługuje pliki cookies.

   Cookies to pliki tekstowe, które przechowywane są w urządzeniu końcowym (np. telefon, tablet lub komputer) używanym przez Użytkownika i przeznaczone są do korzystania ze strony internetowej Banku oraz systemu db hipoNET za pośrednictwem sieci internet. Cookies nie zawierają żadnych programów oraz same w sobie nie są programami. Nie mogą w związku z tym zawierać wirusów, ani nie mogą być wirusami.

   Ograniczenia w stosowaniu plików cookies mogą wpłynąć na niektóre funkcjonalności dostępne na stronie internetowej Banku oraz w db hipoNET, przy czym zablokowanie automatycznej obsługi plików cookies w ustawieniach przeglądarki internetowej spowoduje brak możliwości korzystania z db hipoNET. Treść Polityki Plików Cookies dostępna jest w formacie ogólnodostępnym na stronie internetowej Banku.

3. Nigdy nie wyrażaj zgody na zapisywanie NIKu oraz Kodu Dostępu przez przeglądarkę.

   Zalecane jest przez Bank wyłączenie funkcji zapamiętywania haseł oraz formularzy w przeglądarce internetowej. Jeżeli funkcja zapamiętywania haseł i formularzy pozostanie włączona, przy logowaniu do systemu db hipoNET NIK oraz Kod Dostępu są automatycznie wpisywane. Wyłączenie tej opcji uniemożliwi zalogowanie się do systemu innym osobom.
   - Microsoft Edge → Ustawienia → Profile → Hasła → odznacz „Autowypełnianie haseł"
   - Google Chrome → Więcej narzędzi → Wyczyść dane przeglądania → w sekcji „Zaawansowane" – zaznacz pole „Autouzupełnianie danych formularzy".

4. Sprawdzaj, czy certyfikat serwera nie został cofnięty, co objawia się wyświetleniem symbolu otwartej kłódki przy adresie strony bądź zmianą tła w pasku adresu na kolor czerwony. Nie zapisuj szyfrowanych stron na dysku, aby uniknąć nieuprawnionego przekierowania na inne strony.
5. Aby zapewnić poprawne funkcjonowanie przeglądarki, usuwaj pliki tymczasowe, które są zapisywane w pamięci podręcznej.
   - Microsoft Edge → Ustawienia → Pliki cookie i uprawnienia witryny → Zarządzaj plikami cookie i danymi witryn oraz usuwaj je.
   - Google Chrome → Menu „Ustawienia Google Chrome" → „Narzędzia" → „Wyczyść dane przeglądania…" – wybierz opcję „Opróżnij pamięć podręczną" oraz „Usuń pliki cookie i inne dane witryn" i naciśnij przycisk „Wyczyść dane przeglądarki". Możesz też wskazać okres, z którego zostanie usunięta pamięć podręczna.
6. Nie ignoruj ostrzeżeń prezentowanych w oknie przeglądarki internetowej.

   W nowych wersjach popularnych przeglądarek dostępne są specjalne narzędzia sprawdzające, czy wyświetlona strona internetowa nie ma na celu wyłudzenia poufnych informacji. Są to tak zwane filtry anty-phishingowe. Nie dają one pełnej gwarancji, że dana strona jest na pewno bezpieczna, pozwalają jednak ograniczyć ryzyko kradzieży poufnych danych. Zalecane jest przez Bank włączenie ochrony anty-phishingowej:

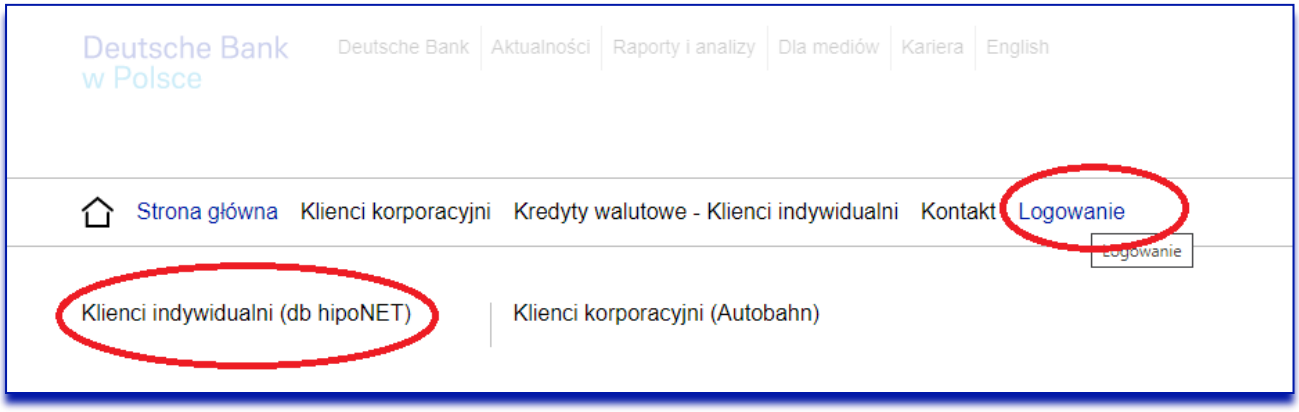
- Microsoft Internet Explorer → „Narzędzia” → w opcji „Filtr witryn wyłudzających informacje” wybierz „Włącz automatyczne sprawdzanie sieci Web”.
- Mozilla Firefox → „Narzędzia” → „Opcje” → w zakładce „Bezpieczeństwo” zaznacz opcje: „Ostrzegaj, jeśli witryny próbują zainstalować dodatki”; „Blokuj witryny zgłoszone jako stwarzające zagrożenie” oraz „Blokuj witryny zgłoszone jako próby oszustwa internetowego”.

7. Używaj nawigacji z menu systemu db hipoNET w celu przechodzenia pomiędzy poszczególnymi funkcjami. Nie używaj opcji „Wstecz”, ani „Dalej” w oknie przeglądarki.

Bezpieczne Logowanie

Loguj się bezpiecznie!

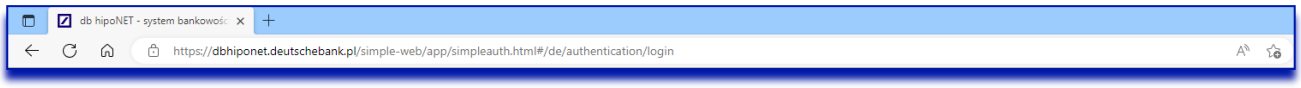
1. Zawsze loguj się poprzez stronę internetową: https://country.db.com/poland lub wpisuj ręcznie w oknie przeglądarki adres: https://dbhiponet.deutschebank.pl/.



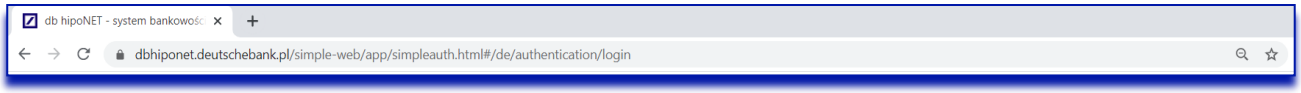
2. Nigdy nie loguj się za pośrednictwem linków otrzymanych w wiadomości e-mail.
3. Nie używaj wyszukiwarek internetowych do znalezienia strony logowania do systemu transakcyjnego Banku.
4. Pamiętaj, że Bank nigdy nie prosi podczas logowania o instalację certyfikatów lub dodatkowego oprogramowania na komputerach lub urządzeniach mobilnych.
5. Komunikacja między urządzeniem Użytkownika, a serwerem Banku szyfrowana jest protokołem TLS. Potwierdzeniem bezpiecznego (szyfrowanego) połączenia jest adres URL rozpoczynający się od https (zamiast standardowego http), gdzie „s” oznacza „secure” – bezpieczny. Upewnij się, że adres strony zaczyna się od liter „https”, a nie „http”.

   Sprawdzaj, czy na stronie logowania (w pasku adresu lub na dole strony) widoczny jest symbol zamkniętej kłódki.

   Najnowsze przeglądarki obok paska adresu wyświetlają informacje o instytucji, dla której został wystawiony certyfikat.



Zrzut ekranu wykonany w przeglądarce Microsoft Edge

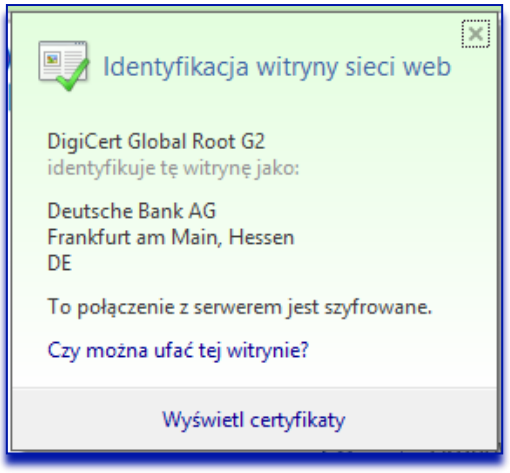


Zrzut ekranu wykonany w przeglądarce Chrome

Zrzut ekranu wykonany w przeglądarce Mozilla Firefox.

Kliknij dwukrotnie w kłódkę, aby sprawdzić czy wyświetlany certyfikat jest ważny i czy został wydany dla Deutsche Bank AG.

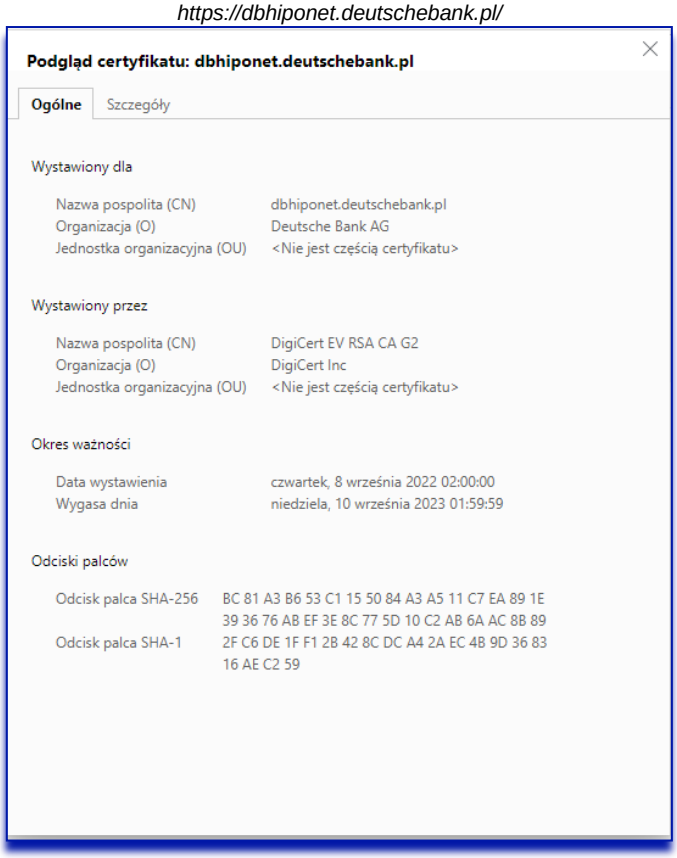
https://dbhiponet.deutschebank.pl/



Sprawdzaj ważność certyfikatu. W tym celu kliknij na wspomniany wyżej symbol zamkniętej kłódki.

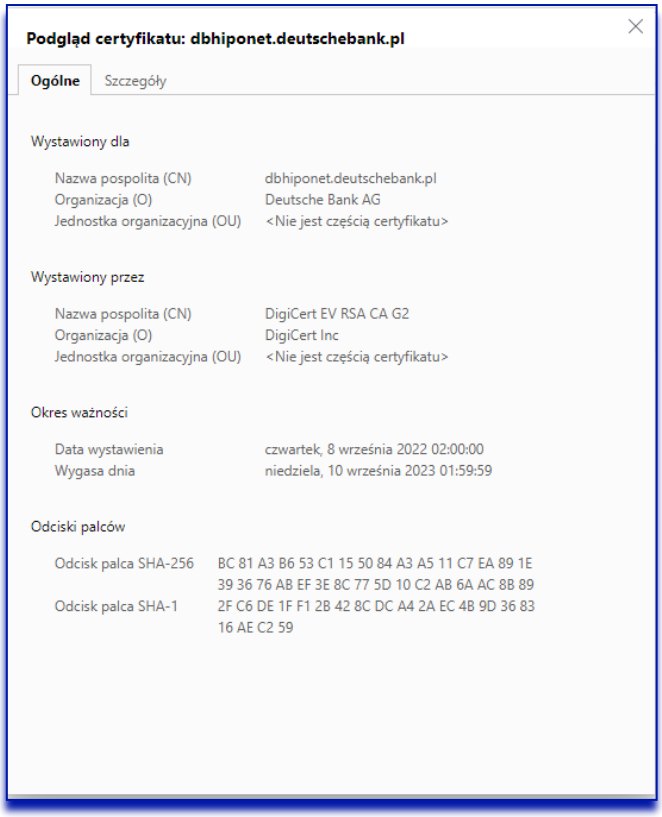
Poprawny certyfikat dla db hipoNET wygląda następująco:

https://dbhiponet.deutschebank.pl/



Zrzut ekranu wykonany w przeglądarce Microsoft Edge

https://dbhiponet.deutschebank.pl/



Zrzut ekranu wykonany w przeglądarce Microsoft Edge

Jeśli zauważysz co najmniej jeden z poniższych objawów:

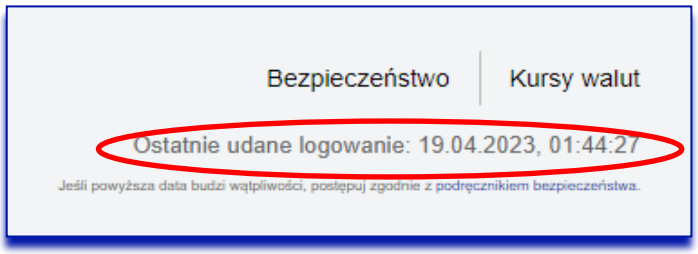
- Kłódka widoczna na pasku adresu strony nie jest zamknięta lub pojawia się przy niej symbol ostrzeżenia.
- Certyfikat jest nieważny lub został wystawiony dla instytucji innej niż Deutsche Bank AG.
- Odcisk certyfikatu – „Odcisk palca" (Thumbprint, Fingerprint) powinien być zgodny ze wskazanym powyżej.
- Strona Internetowej Obsługi Kredytu db hipoNET przed lub po zalogowaniu wygląda inaczej, lub prezentuje inne komunikaty niż zazwyczaj.
- Proces logowania do db hipoNET wygląda inaczej niż zwykle (pojawiają się inne okna, trwa dłużej niż zazwyczaj, pojawiają się prośby o podanie dodatkowych danych).

Przerwij logowanie i niezwłocznie skontaktuj się z pracownikiem Banku!

Opisane wyżej sytuacje oraz wszystkie przypadki niezgodności daty i godziny logowania do systemu zgłoś jak najszybciej pracownikom Banku (dzwoniąc pod numery: 801 103 103* lub +48 22 4 680 680* w dni robocze w godzinach: 9:00-17:00).

** Opłata za połączenia telefoniczne wg obowiązujących stawek operatora.*

6. Podczas wpisywania Numeru Identyfikacyjnego Klienta oraz Kodu Dostępu zwracaj uwagę, czy nikt nie podgląda wpisywanych danych.
7. Po poprawnym zalogowaniu się do systemu, sprawdź każdorazowo, czy data ostatniego logowania (informacja dostępna w prawym dolnym rogu ekranu systemowego db hipoNET) jest właściwa.



8. Po zakończeniu pracy w db hipoNET zawsze używaj opcji „Wyloguj" zlokalizowanej w prawym górnym rogu ekranu systemowego.

Ochrona Numeru Identyfikacyjnego Klienta (NIK) oraz Kodu Dostępu

1. Nie ujawniaj osobom trzecim danych służących do logowania do systemu (NIKu, Kodu Dostępu).
2. Jeśli podejrzewasz, że ktoś może znać Twój Kod Dostępu – natychmiast dokonaj jego zmiany. Możesz to zrobić bezpośrednio w systemie db hipoNET.
3. Okresowo dokonuj zmiany swojego Hasła. Zadbaj, żeby nie składało się ono z informacji, które w jakiś sposób mogą być z Tobą skojarzone (np. data urodzenia, imię itp.). Bank rekomenduje zmianę hasła co 90 dni.
4. Nie przesyłaj nigdy poufnych danych (takich jak NIK, Kod Dostępu) drogą e-mailową.
5. Staraj się nie zapisywać NIKu oraz Kodu Dostępu ani w formie papierowej, ani elektronicznej. Jeśli jednak konieczny jest zapis tego typu – korzystaj z programów do zapamiętywania haseł oferowanych przez znanych dostawców.
6. Nie zapisuj poufnych danych na stałe w pamięci przeglądarek internetowych (patrz. Konfiguracja przeglądarki).

Zabezpieczenia zastosowane w systemie db hipoNET

Numer Identyfikacyjny Klienta (NIK) i Kod Dostępu

Uwierzytelnienie użytkownika podczas logowania do systemu db hipoNET odbywa się po podaniu unikalnego Numeru Identyfikacyjnego Klienta oraz Kodu Dostępu do systemu.

Numer Identyfikacyjny Klienta (NIK) – to 10-cyfrowy numer, który otrzymałeś drogą korespondencyjną z Banku.

Kod Dostępu do db hipoNET – jest to poufny ciąg znaków alfanumerycznych, zawierający minimalnie 8 znaków spełniający przynajmniej trzy wybrane elementy z następujących: cyfra, wielka litera, mała litera, znak specjalny.

Podczas pierwszego logowania do nowego systemu db hipoNET (od 24.04.2023 r.) należy wprowadzić dotychczasowy Kod Dostępu poprzedzony prefixem "**DB!**" (przykład: dotychczasowy Kod Dostępu "12345678", nowy Kod Dostępu "DB!12345678"). Następnie system wymusi ustawienie nowego Kodu Dostępu, z wykorzystaniem liter, cyfr i znaków specjalnych.

W przypadku zmiany lub nadania nowego Kodu Dostępu do db hipoNET za pomocą Serwisu Telefonicznego podczas połączenia zostanie wygenerowany przez Ciebie 8-cyfrowy Kod inicjalny, który ze względów bezpieczeństwa nie może zawierać obok siebie trzech identycznych znaków oraz ciągu kolejnych cyfr w porządku rosnącym bądź malejącym. Kod powinien składać się przynajmniej z trzech różnych cyfr oraz nie może być taki sam jak poprzednie dziesięć Kodów Dostępu. Podczas pierwszego logowania po zmianie Kodu Dostępu w Serwisie Telefonicznym – kod inicjalny należy poprzedzić prefixem „**DB!**”, następnie system wymusi ustawienie nowego Kodu Dostępu, z wykorzystaniem liter cyfr i znaków specjalnych.

W przypadku zmiany Kodu Dostępu do db hipoNET za pomocą systemu Internetowej Obsługi Kredytu (Ustawienia → Zmiana hasła → Ustaw nowe hasło) należy wpisać nowy Kod Dostępu zawierający co najmniej 8 znaków, w tym przynajmniej trzy wybrane elementy z następujących: cyfra, wielka litera, mała litera, znak specjalny.

Pamiętaj, że możesz wzmocnić zabezpieczenie poprzez zastosowanie kilku prostych zasad. Kod Dostępu do db hipoNET nie powinien:

- stanowić składowej NIK,
- zawierać sekwencji kolejnych liter, liczb lub innych,
- zawierać bezpośrednio kojarzących się z Twoją osobą dat i słów (daty Twojego urodzenia, dat ważnych dla Twoich bliskich, Twojego imienia, nazwiska, imion bliskich i zwierząt itp.) być hasłem wykorzystywanym w innych witrynach internetowych.

Kod Dostępu do Serwisu Telefonicznego – to 8-cyfrowy kod, znany jedynie Tobie, który wygenerowany został przez Ciebie podczas połączenia z Serwisem Telefonicznym świadczonym przez Wirtualny Oddział pod nr tel. 801 103 103* lub +48 22 4 680 680* (w dni robocze, w godz. 9-17).

Pamiętaj, że możesz wzmocnić zabezpieczenie poprzez zastosowanie kilku prostych zasad. Kod Dostępu do Serwisu Telefonicznego nie powinien:

- stanowić składowej NIK,
- zawierać w sobie ciągów takich samych cyfr,
- zawierać bezpośrednio kojarzących się z Twoją osobą dat (daty Twojego urodzenia, dat ważnych dla Twoich bliskich itp.).

** Opłata za połączenia telefoniczne wg obowiązujących stawek operatora*

Sytuacje alarmowe

Jeśli stwierdzisz zaistnienie jednego z poniższych przypadków:

- próba zalogowania się do Internetowej Obsługi Kredytu db hipoNET przez osoby do tego nieuprawnione,
- podejrzenie przechwycenia przez osobę/osoby nieuprawnioną/nieuprawnione danych do logowania,

skontaktuj się z Bankiem, dzwoniąc pod numery: 801 103 103* lub +48 22 4 680 680* (w dni robocze w godzinach 9:00-17:00). Po przedstawieniu naszemu pracownikowi zaistniałego problemu, postępuj zgodnie z jego wskazówkami.

Dodatkowo w sytuacji, gdy sprawa związana jest z podejrzeniem włamania do Internetowej Obsługi Kredytu db hipoNET, jak najszybciej zmień Kod Dostępu do systemu (możesz to zrobić w db hipoNET wybierając Ustawienia → Zmiana hasła → Ustaw nowe hasło).

** Opłata za połączenia telefoniczne wg obowiązujących stawek operatora.*