

Bezpieczeństwo i jakość usług bankowości internetowej – protokół TLS 1.2

Co to jest TLS?

TLS (z ang. Transport Layer Security) - zapewnia poufność i integralność transmisji danych, a także uwierzytelnienie serwera, a niekiedy również klienta poprzez zastosowanie mechanizmu szyfrowania.

Obecnie standardem obsługiwanym przez większość z popularnych przeglądarek internetowych jest protokół TLS w wersji 1.2, zapewniający wyższy poziom ochrony niż jego niższe wersje (tj. TLS 1.0 i TLS 1.1).

Czy wszystkie przeglądarki internetowe obsługują protokół TLS 1.2?

Protokół TLS 1.2 obsługiwany jest jedynie przez nowsze wersje przeglądarek internetowych. W większości z najnowszych wersji przeglądarek internetowych, obsługa TLS 1.2 jest automatycznie włączona. W niektórych starszych wersjach przeglądarek, obsługa protokołu jest możliwa, ale wymaga modyfikacji ustawień przeglądarki w tym zakresie przez użytkownika (tj. „ręcznego” włączenia obsługi protokołu TLS 1.2).

Problem z obsługą protokołu TLS 1.2 mogą mieć w szczególności użytkownicy sprzętu wyposażonego w systemy operacyjne pozbawione wsparcia dostawców – m.in. Windows XP (bez Service Pack 3) i inne starsze wersje systemu Windows (95, 98, czy VISTA) oraz systemu Android w wersji niższej niż 4.1.

Jak sprawdzić czy przeglądarka internetowa obsługuje protokół TLS 1.2?

W większość aktualnych wersji najpowszechniejszych na rynku przeglądarek internetowych obsługa protokołu TLS 1.2 jest automatycznie włączona.

Niemniej jednak, celem potwierdzenia odpowiedniego poziomu bezpieczeństwa, należy dokonać weryfikacji poprawności ustawień.

Microsoft Internet Explorer:

1. Aby sprawdzić, czy protokół TLS 1.2. jest włączony, wybierz w **Menu przeglądarki** → **Narzędzia** → **Opcje internetowe** → zakładkę „**Zaawansowane**”.
2. Przewiń suwakiem w dół i w kategorii „**Zabezpieczenia**” upewnij się, że włączone jest ustawienie „**Użyj szyfrowania TLS 1.2**”.
3. Jeżeli ustawienie nie jest włączone, zaznacz ustawienie i wybierz przycisk OK. Zamknij i ponownie uruchom przeglądarkę Internet Explorer.

Google Chrome:

Jeśli przeglądarka Google Chrome jest w wersji wyższej niż 30, to protokół TLS 1.2 jest automatycznie włączony.

Aby sprawdzić wersję i aktualność przeglądarki Google Chrome:

1. Otwórz przeglądarkę **Google Chrome**.
2. Kliknij w ikonę **menu** w prawym rogu przeglądarki.
3. Wybierz **Pomoc** → **Google Chrome** → **informacje**.
4. Jeżeli zweryfikowana wersja przeglądarki jest niższa niż 30 należy dokonać jej niezwłocznej aktualizacji.

Mozilla Firefox:

Jeśli przeglądarka Mozilla Firefox jest w wersji 27 lub wyższej, to protokół TLS 1.2 jest domyślnie włączony.

Aby sprawdzić wersję i aktualność Mozilla Firefox:

1. Otwórz przeglądarkę **Mozilla Firefox**.
2. Kliknij w ikonę **menu** w prawym rogu przeglądarki.
3. Wybierz ikonę **Pomoc**, a następnie **O programie Firefox**.
4. Jeżeli zweryfikowana wersja przeglądarki jest niższa niż 27 należy dokonać jej niezwłocznej aktualizacji.

Opera:

Jeśli przeglądarka Opera jest w wersji 17 lub wyższej, to protokół TLS 1.2 jest zawsze włączony.

Aby sprawdzić wersję i aktualność przeglądarki Opera:

1. Otwórz przeglądarkę **Opera**.
2. Kliknij **Menu** w lewym górnym rogu przeglądarki.
3. Wybierz **Opera – informacje**.
4. Jeżeli zweryfikowana wersja przeglądarki jest niższa niż 17 należy dokonać jej niezwłocznej aktualizacji.

Apple Safari OS X

Jeśli używasz przeglądarki Safari dla MacOS w wersji 7 lub nowszej, protokoły zabezpieczeń TLS 1.1 i TLS 1.2 są włączone automatycznie.

W przeglądarce Safari nie można zmieniać ustawień protokołów połączenia szyfrowanego.

Szczegółowe informacje na temat kompatybilnych przeglądarek internetowych można znaleźć na stronie <https://caniuse.com> (w polu wyszukiwarki na stronie należy wpisać TLS 1.2).