Bezpieczeństwo usług oraz informacje o certyfikatach

Klienci banku powinni stosować się do poniższych zaleceń:

- nie przechowywać danych dotyczących swojego konta w jawnej postaci w miejscu, z którego mogą być w prosty sposób skradzione bądź ujawnione osobom postronnym,
- nie przesyłać danych wykorzystywanych do obsługi kont bankowych przez e-mail, telefon, gdyż **banki nigdy nie proszą o podanie danych poufnych drogą elektroniczną**, a nadawca takich wiadomości, podszywając się zwykle pod zaufaną firmę lub osobę, ma na celu wyłudzenie poufnych informacji (numery kart kredytowych, hasła do systemów bankowych, hasła portali aukcji internetowych),
- korzystać z nowoczesnych narzędzi ostrzegających przed wejściem na strony stworzone w celu wyłudzenia poufnych danych. Nowe wersje popularnych przeglądarek posiadają filtry ***antyphishingowe*** (specjalne narzędzia sprawdzające, czy wyświetlona strona internetowa nie ma na celu wyłudzenia poufnych informacji). Programy te nie dają, co prawda, pełnej gwarancji, że dana strona jest bezpieczna, pozwalają jednak znacznie ograniczyć ryzyko utraty danych służących uwierzytelnianiu,
- korzystać z usług bankowości internetowej wyłącznie przy użyciu znanego sobie sprzętu, gdyż podstawowym zagrożeniem występującym w ogólnodostępnych systemach jest możliwość instalacji „złośliwego" oprogramowania przez osoby uprzednio korzystające z danego stanowiska,
- każdorazowo podczas logowania zwracać uwagę na datę ostatniego logowania do systemu,
- nie otwierać i nie uruchamiać plików oraz programów nieznanego pochodzenia oraz ze szczególną ostrożnością traktować programy pobierane z Internetu. Wiele darmowych programów dostępnych w sieci zawiera moduły szpiegujące (***ang. spyware***), które dostarczają ich autorom cennych informacji o użytkowniku - głównie **adres IP**, używany **system operacyjny**, przeglądarkę, a niekiedy strony, z którymi się łączył użytkownik. Aplikacje typu ***spyware*** mogą umożliwić osobom niepowołanym śledzenie danych wpisywanych przez użytkownika w przeglądarce internetowej, w tym również numer klienta, PIN, numery kart płatniczych itd.,
- zwracać uwagę na symptomy zainfekowania komputera, takie jak: spowolnienie działania systemu, spowolnienie transferu, zwiększona liczba reklam, zmiany w działaniu przeglądarki internetowej, problemy z działaniem niektórych programów,
- nie klikać na podejrzane odnośniki podawane w e-mailu,
- po każdym wykryciu i usunięciu wirusa lub konia trojańskiego zmieniać PIN do usługi oraz wszelkie hasła dostępu,
- nie uruchamiać programów nieznanego pochodzenia przesyłanych pocztą elektroniczną
- posiadać aktualne wersje przeglądarek internetowych, uaktualniać na bieżąco system operacyjny, używać aktualnego oprogramowania antywirusowego

Bezpieczeństwo usług dostępnych poprzez Internet

Dla zapewnienia jak najwyższego poziomu bezpieczeństwa przy wymianie informacji z klientem wykorzystuje się protokół szyfrujący Secure Socket Layer (SSL). Protokół SSL zapewnia poufność informacji i gwarantuje, że nikt postronny nie może odczytać lub zmienić danych przesyłanych między klientem a bankiem.
W trakcie połączenia ze stronami naszego Banku używane są następujące techniki kryptograficzne:
Algorytm symetryczny, używany do zabezpieczenia całej sesji komunikacyjnej między przeglądarką klienta a serwerem WWW - stosowany klucz symetryczny ma 128/256 bitów –jest dedykowany dla operacji finansowych

Algorytm asymetryczny (z kluczem prywatnym i publicznym serwera banku), używany w czasie inicjacji połączenia do zabezpieczenia transmisji losowo wygenerowanego klucza sesyjnego (wykorzystywanego w algorytmie symetrycznym);

Klucz publiczny Centrum Usług Internetowych ma **2048** bity

Bank Spółdzielczy w Oleśnicy posiada certyfikaty do swoich stron szyfrowanych:

- *Serwis WWW https://www.bsolesnica.pl*
  Szczegóły certyfikatu:
  Wystawca: **Certum Extended Validation CA SHA2**
  Numer seryjny: **71:3F:9D:6D:44:B9:8C:DE:2C:3A:CD:5D:7B:FF:52:B1**
  Odcisk SHA1: **82:8D:B2:B1:7D:7B:5B:7B:FC:C0:0F:B2:F5:17:EC:99:6B:4A:D2:E6**
  Ważny od: **czwartek, 19 maja 2016**
  Ważny do: **sobota, 19 maja 2018**

  klienci KORPORACYJNI:
- Serwis Bankowości Internetowej – https://bank.cui.pl/olesnica_k
  Szczegóły certyfikatu:
  Wystawca: **thawte SSL CA - G2**
  Numer seryjny: **52:E6:23:1D:AD:89:BD:48:37:E1:DB:1E:B6:BC:12:74**
  Odcisk SHA1: **A2:D2:49:05:6B:E6:09:3B:23:9E:A0:E4:E9:3A:D1:C7:24:F3:B4:28**
  Ważny od: **poniedziałek, 14 września 2015**
  Ważny do: **piątek, 14 października 2016**

  klienci INDYWIDUALNI
- Serwis Bankowości Internetowej – https://bank.cui.pl/olesnica
  Szczegóły certyfikatu:
  Wystawca: **thawte SSL CA - G2**
  Numer seryjny: **52:E6:23:1D:AD:89:BD:48:37:E1:DB:1E:B6:BC:12:74**
  Odcisk SHA1: **A2:D2:49:05:6B:E6:09:3B:23:9E:A0:E4:E9:3A:D1:C7:24:F3:B4:28**
  Ważny od: **poniedziałek, 14 września 2015**
  Ważny do: **piątek, 14 października 2016**

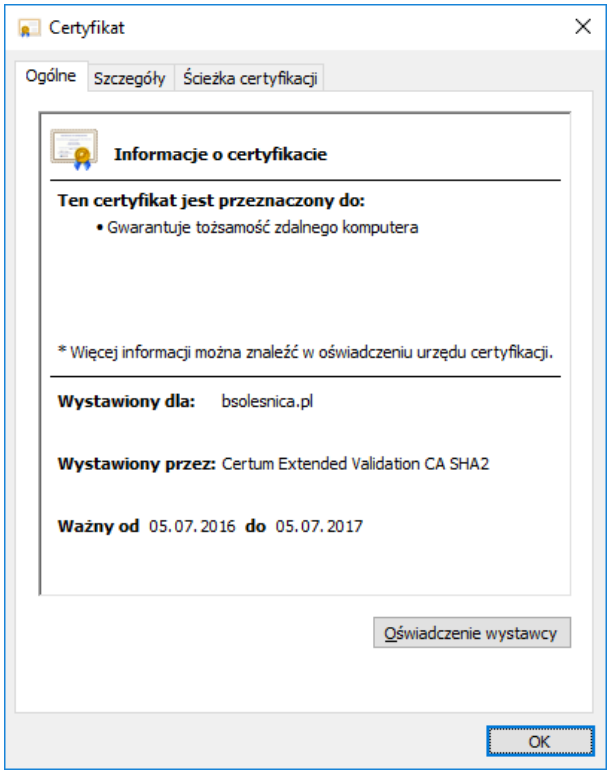
- Nowy Serwis Bankowości Internetowej (CBP)– https://bsolesnica.net/
  Szczegóły certyfikatu:
  Wystawca: **Certum Extended Validation CA SHA2**
  Numer seryjny: **2A:C5:E7:23:55:F5:E5:3E:D7:B2:9B:2F:03:19:A3:6C**
  Odcisk SHA1: **E5:AC:9B:0B:DE:ED:CA:0A:2A:99:9A:61:F1:CD:CF:38:7C:C9:05:04**
  Ważny od: **czwartek, 19 maja 2016**
  Ważny do: **sobota, 19 maja 2018**

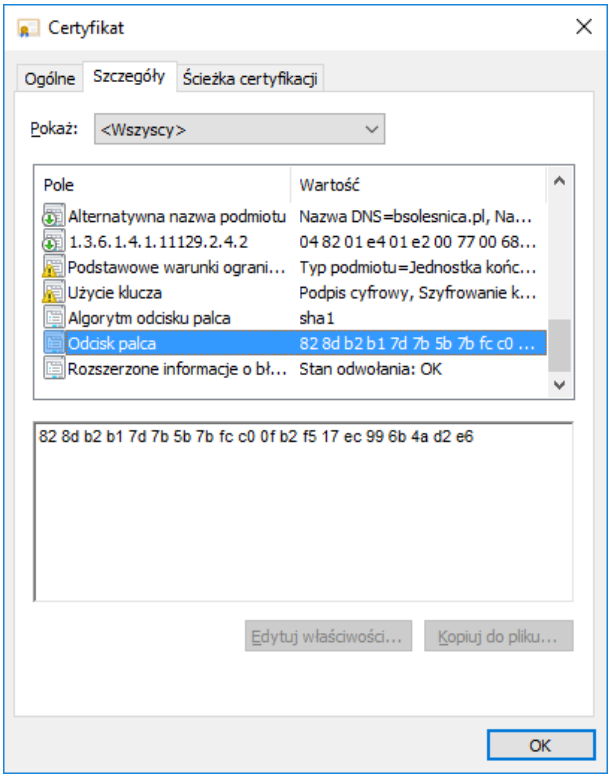
Sprawdzenia włączonego szyfrowania oraz długości klucza użytego do niego można dokonać ustawiając wskaźnik myszy na odpowiednim polu przeglądarki internetowej.
Poniżej przedstawiamy dwie przykładowe lokalizacje opisów certyfikatów w popularnych przeglądarkach:

Wyświetlenie szczegółów certyfikatu w przeglądarce Internet Explorer:

Klikając na symbol kłódki w pasku adresu można otworzyć okienko z podstawowymi informacjami dotyczącymi certyfikatu.

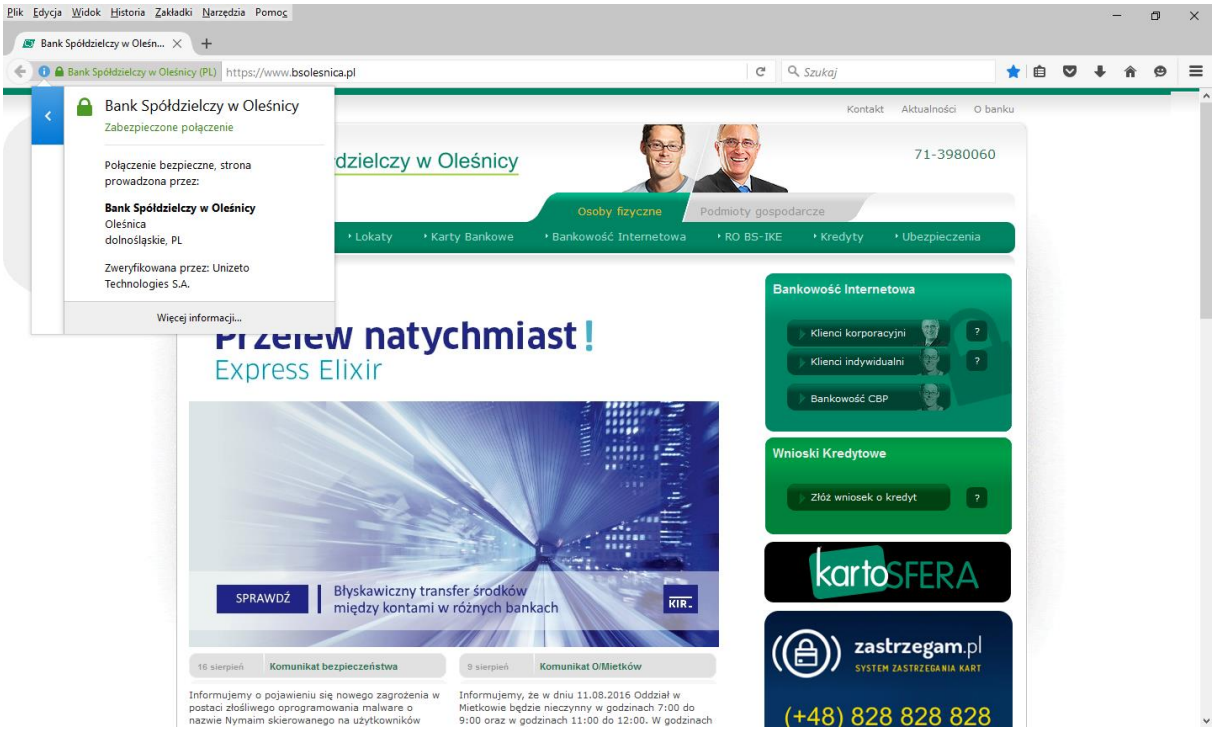
Więcej informacji o używanym certyfikacie otrzymamy wybierając opcję „Wyświetl certyfikat”, zakładka „Szczegóły”.
Na tym etapie proszę o weryfikację odcisku palca (wg Algorytm odcisku palca: SHA1) oraz datę ważności certyfikatu.



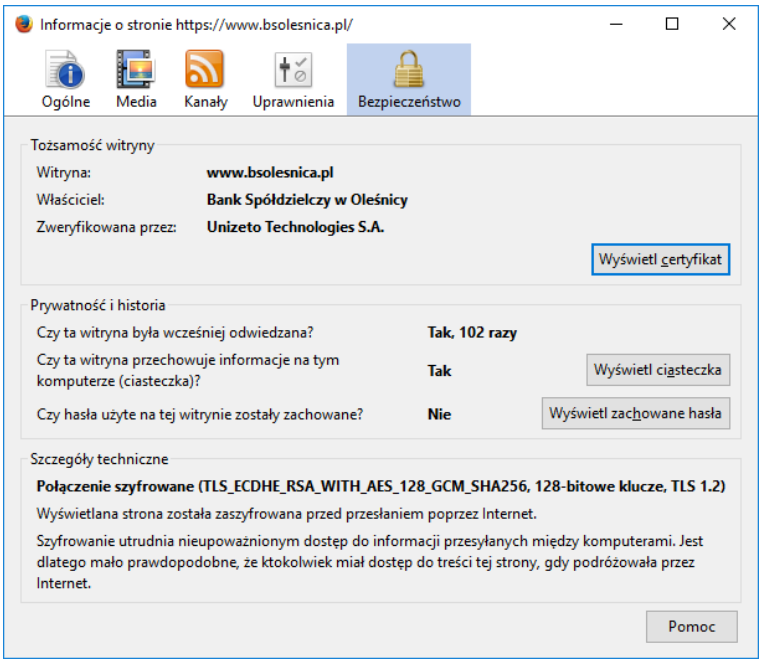


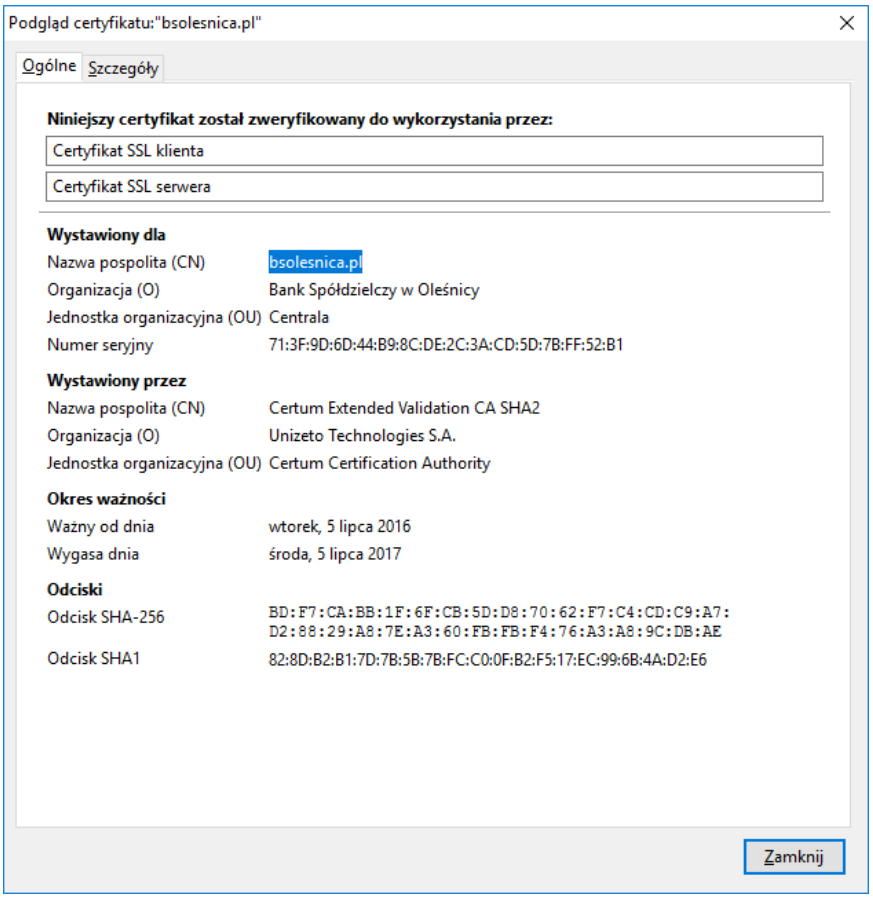
Wyświetlenie szczegółów certyfikatu w przeglądarce Mozilla Firefox:

Klikając na symbol kłódki w pasku adresu można otworzyć okienko z podstawowymi informacjami dotyczącymi certyfikatu.



Więcej informacji o używanym certyfikacie otrzymamy wybierając opcję „Więcej informacji", zakładka „Bezpieczeństwo" -> „wyświetl certyfikat"
Na tym etapie proszę o weryfikację odcisku SHA1 oraz datę ważności certyfikatu.




Podgląd certyfikatu:"bsolesnica.pl"
Ogólne
Szczegóły
Niniejszy certyfikat został zweryfikowany do wykorzystania przez:
Certyfikat SSL klienta
Certyfikat SSL serwera
Wystawiony dla
Nazwa pospolita (CN) bsolesnica.pl
Organizacja (O) Bank Spółdzielczy w Oleśnicy
Jednostka organizacyjna (OU) Centrala
Numer seryjny 71:3F:9D:6D:44:B9:8C:DE:2C:3A:CD:5D:7B:FF:52:B1
Wystawiony przez
Nazwa pospolita (CN) Certum Extended Validation CA SHA2
Organizacja (O) Unizeto Technologies S.A.
Jednostka organizacyjna (OU) Certum Certification Authority
Okres ważności
Ważny od dnia wtorek, 5 lipca 2016
Wygasa dnia środa, 5 lipca 2017
Odciski
Odcisk SHA-256 BD:F7:CA:BB:1F:6F:CB:5D:D8:70:62:F7:C4:CD:C9:A7:D2:88:29:A8:7E:A3:60:FB:FB:F4:76:A3:A8:9C:DB:AE
Odcisk SHA1 82:8D:B2:B1:7D:7B:5B:7B:FC:C0:0F:B2:F5:17:EC:99:6B:4A:D2:E6
Zamknij