Moduł 1.

Wykorzystanie internetowych technologii komunikacyjnych

Rozdział 5.

Bezpieczeństwo komunikacji

Zajęcia 5.

2 godziny

Nauczymy się:

- Rozróżniać szyfrowanie symetryczne i asymetryczne.
- Sprawdzać, czy połączenie korzysta z jawnego http, czy zabezpieczonego https.
- Sprawdzać szczegóły certyfikatu stosowanego do zabezpieczenia komunikacji https.
- Pobierać i instalować certyfikat.
- Odróżniać podpis kwalifikowany od niekwalifikowanego.
- Nawiązywać połączenie VPN.

Praktyczne zastosowanie zdobytej wiedzy

Zdobyta wiedza pozwoli świadomie korzystać z komunikacji zabezpieczonej SSL, a także weryfikować wiarygodność certyfikatu zabezpieczającego komunikację

Omówienie zagadnienia

W trakcie nawiązywania połączenia przez sieć internetową, należy zwrócić uwagę na bezpieczeństwo naszych danych. Obecnie najpopularniejszym sposobem przesyłania danych w Internecie są strony internetowe. Sposób porozumiewania się pomiędzy komputerami określa protokół, podobnie jak język określa metodę komunikacji poprzez rozmowę między ludźmi. Ten protokół to HTTP. Jednak „rozmowę" komputerów może ktoś „podsłuchać" i, jeśli zna język http, wtedy mógłby dowiedzieć się wielu informacji, które dla nas są poufne (np. login i hasło).

Kiedy piszemy do kogoś list i chcemy zachować prywatność, możemy go zaszyfrować. Ustalamy, że będziemy wykorzystywać

– **uporządkowane litery**: aąbcćdeęfghijklłmnńoópqrsśtuvwxyzźż,

– i **uporządkowane cyfry**: 0123456789.

Definiujemy, że każda litera będzie przesunięta o określoną wartość klucza wg alfabetu – np. gdy klucz wynosi 1, zamiast litery 'b' piszemy 'c', zamiast litery 's' piszemy 't', zamiast 'ż' stawiamy 'a' itd. Zatem użyjemy jako algorytmu prostego przesunięcia.

Zasada, która określa, że następuje przesunięcie o wartość klucza to algorytm, wartość przesunięcia to klucz. Zaprezentowany algorytm jest bardzo słaby, w praktyce wykonywane działania (algorytm) są znacznie bardziej skomplikowane, niż przedstawione dodanie wartości klucza do znaku. Taki sposób szyfrowania, gdy jest to działanie odwracalne do szyfrowania z wykorzystaniem tego samego klucza, nazywamy szyfrowaniem symetrycznym.

W podanym wcześniej przykładzie ustaliliśmy, że kluczem jest 1, przesyłamy tekst „tajne", a szyfrowanie: t + 1 = u; a + 1 = ą, j + 1 = k, n + 1 = ń, e + 1 = ę, zatem zaszyfrowany tekst: „uąkńę".

Osoba, która otrzymała zakodowany list wykona działanie odwrotne z wykorzystaniem znanego wcześniej klucza:

– zaszyfrowany tekst „uąkńę"

– wiemy, że algorytm polega na przesunięciu o znaną wartość klucza

– wiemy, że klucz ma wartość 1

– odszyfrowanie poprzez działanie odwrotne: u – 1 = t, ą – 1 = a, k – 1 = j, ń – 1 = n, ę – 1 = e

– odszyfrowana wiadomość: „tajne".

Szyfrowanie symetryczne wykorzystuje stosunkowo prosty mechanizm matematyczny, dzięki czemu komputery mogą takie działania wykonać dosyć szybko. Podstawowym problemem szyfrowania symetrycznego jest bezpieczna wymiana klucza przed rozpoczęciem szyfrowania asymetrycznego.

Trudność tę rozwiązały wymyślone w latach 70. zeszłego wieku matematyczne podstawy szyfrowania matematycznego (na ten temat zobacz w Internecie np. artykuł dostępny na stronie internetowej: http://www.mimuw.edu.pl/~czarnik/zajecia/bezp09/W02-wprowadzenie2.pdf).

Aby przedstawić sposób szyfrowania asymetrycznego, wyobraźmy sobie następującą sytuację. Dwie osoby chcą bezpiecznie wymieniać klucz szyfrujący. Każda z nich zakłada sobie sejf wrzutkowy. Sejf jest ustawiony w miejscu publicznym i każdy może wrzucić do niego list, ale tylko właściciel sejfu posiada klucz pozwalający wyjąć listy. Chcąc bezpiecznie przekazać wiadomość, udajemy się do sejfu, piszemy wiadomość, a następnie wrzucamy list do sejfu. Po tym fakcie nie mamy już do niego dostępu, tylko właściciel posiadający do niego prywatny klucz może go otworzyć. Dlatego takie szyfrowanie nazywamy asymetrycznym. Problemem jest wysoki koszt korzystania z szyfrowania asymetrycznego i jego jednokierunkowość.

Mechanizm ten jest zazwyczaj wykorzystywany do bezpiecznego przekazania klucza do szyfrowania symetrycznego. Na kartce piszemy słowo zgłoszeniowe i wartość klucza. Następnie dzwonimy do osoby, która wcześniej, korzystając ze swojego klucza symetrycznego, odebrała bezpiecznie przekazane jej wiadomości. Na początku rozmowy podajemy słowo zgłoszeniowe, co pozwala znaleźć odpowiedni klucz. Dalej, choćby w rozmowie telefonicznej, można w sposób bezpieczny przekazywać sobie wiadomości. Jednak gdy długo wykorzystujemy ten sam klucz, istnieje ryzyko jego złamania.

Ktoś podsłuchał wiadomość. Sprawdza co otrzyma, gdy użyje rożnych kluczy:

...gdyby kluczem było 100, to dla liter 100 mod 35 = 30, reszta z dzielenia jest kluczem, więc dla liter jest 35 kluczy (około 5 bitów), dla cyfr jest 10 kluczy (około 4 bitów);

...gdyby kluczem było 4:

uąkńę: u – 4 = r, ą – 4 = z, k – 4 = g, ń – 4 = l, ę – 4 = c

otrzymujemy: śżimd, czyli bez sensu;

...gdyby kluczem było 3:

uąkńę: u – 3 = s, ą – 3 = ź, k – 3 = h, ń – 3 = ł, ę – 3 = ć

otrzymujemy: sźhłć, czyli bez sensu;

...gdyby kluczem było 2:

uąkńę: u – 2 = ś, ą – 2 = ż, k – 2 = i, ń – 2 = m, ę – 2 = d

otrzymujemy: śżimd, czyli bez sensu;

...gdyby kluczem było 1:

uąkńę: u – 1 = t, ą – 1 = a, k – 1 = j, ń – 1 = n, ę – 1 = e

otrzymujemy: **tajne**, czyli ma sens.

Każdy znak ma w tzw. tablicy znaków przypisany odpowiedni numer. Istnieje wiele używanych tablic znaków, np. tablica ASCI obejmuje znaki widoczne na klawiaturze i np.: 65 to A, 66 to B, 67 to C, ..., 97 to a, 98 to b, 99 to c itd. (więcej informacji można uzyskać np. na stronie: http://pl.wikipedia.org/wiki/ASCII).

Oczywiście dostępnych jest mnóstwo innych ustalonych sposobów kodowania, czyli przypisywania liczbom określonego znaku np. ISO_8859-2, uwzględniających dodatkowo również polskie litery (więcej informacji można uzyskać np. na stronie internetowej: http://pl.wikipedia.org/wiki/ISO_8859-2).

Polskie litery uwzględnia również standard Windows-1250 (więcej informacji można uzyskać np. na stronie: http://pl.wikipedia.org/wiki/Windows-1250).

Inne przykłady kodowania można uzyskać np. na stronach:
http://pl.wikipedia.org/wiki/Base64
http://pl.wikipedia.org/wiki/Unicode.

Biorąc wartość liczbową każdego znaku zamiast stosować zwykłe przesunięcie możemy wykonać działanie matematyczne. Oczywiście, w miejsce dodawania możemy użyć mnożenia, potęgowania lub złożonych działań matematycznych, co zwiększa liczbę możliwych kombinacji dla bardziej złożonego algorytmu.

Teoretycznie mocnym zabezpieczeniem byłoby używanie tajnego algorytmu. Na tej zasadzie działają niektóre zamknięte algorytmy szyfrowania. Jednak w dobie Internetu i wielu bardzo dociekliwych ludzi (i dużej mocy obliczeniowej komputerów) tajność algorytmu zazwyczaj nie utrzymuje się długo. Poza tym używanie zamkniętych algorytmów zmusza do stosowania produktu określonej firmy. Można próbować zakładać, że im bardziej złożony algorytm, tym trudniej go złamać. Problem w tym, że bardziej kosztowne staje się jego używanie, ponadto wiele złożonych matematycznie algorytmów można skrócić.

Np. przyjmijmy, że

x to wynik szyfrowania,

y dane niezaszyfrowane,

a wartość klucza.

Przyjmijmy algorytm $y = (2a + 2 * 4a - a + 5 * a - 3a) * x$, co po uproszczeniu daje

$y = 11a * x$.....

Opracowanie algorytmu:

- którego nie można uprościć,
- który daje wysoką moc szyfrowania,
- przy niskim koszcie szyfrowania,

jest złożonym zadaniem matematycznym.

Na początku ery komputerów takim algorytmem był DES (Data Encryption Standard), który korzysta z klucza 56-bitowego, co daje 2^{56} kombinacji. Ale przy rosnącej mocy obliczeniowej komputerów obecnie taka liczba kombinacji jest do sprawdzenia w czasie sekund. Jednym z popularniejszych algorytmów jest algorytm AES, który korzysta z klucza 128-bitowego (lub dłuższego), gdzie liczba dostępnych kombinacji sięga 3,4 x 10^{38}. Gdy posiadamy komputer, który może 2^{56} kombinacji klucza 56-bitowego sprawdzić w ciągu 1 sekundy, do sprawdzenia wszystkich kombinacji klucza 128-bitowego potrzebowałby 149 bilionów lat. Moc obliczeniowa komputerów rośnie bardzo szybko, dlatego używa się coraz dłuższych kluczy, obecnie zazwyczaj 2048-bitowych.

Jednak wydłużenie klucza powoduje wzrost kosztu szyfrowania. Ponadto jak omówiliśmy na przykładzie algorytmu prostego przesunięcia dla danego algorytmu istnieje jakaś graniczna długość klucza, gdy wydłużanie klucza nie powoduje wzrostu siły szyfrowania, a jedynie koszt szyfrowania.

W szyfrowaniu transmisji ważne są więc dwa zagadnienia: szyfrowanie symetryczne, które przy stosunkowo niskim koszcie zapewnia silne szyfrowanie w dwie strony, ale istnieje problem bezpiecznego przekazanie klucza, oraz szyfrowanie asymetryczne, gdzie można publiczny klucz szyfrujący (omawiana wcześniej wrzutka) udostępnić wszystkim. Klucz publiczny umożliwia zaszyfrowanie, ale nie można użyć go do odszyfrowania. Do odkodowania danych zaszyfrowanych kluczem publicznym potrzebny jest klucz prywatny.

W szyfrowaniu asymetrycznym stosuje się dwa klucze: publiczny służący do szyfrowania i prywatny służący do odszyfrowania. Cechą szyfrowania asymetrycznego jest kodowanie w jedną stronę. Do szyfrowania w dwie strony potrzebne są dwie pary kluczy, ponieważ każda para zapewnia szyfrowanie w jedną stronę. Jako „pudełka" na parę kluczy używa się zazwyczaj tzw. certyfikatu, o którym za chwilę. Problemem szyfrowania asymetrycznego jest również wykorzystywanie bardzo skomplikowanych działań matematycznych. Nie jest to problemem, gdy szyfrujemy i deszyfrujemy niewielką liczbę danych, jednak przy dużych ilościach stanowi to trudność nawet przy obecnie dostępnej mocy obliczeniowej. Dlatego zazwyczaj stosuje się połączenie obu mechanizmów.

Szyfrowanie asymetryczne pozwala na bezpieczną wymianę klucza do szyfrowania symetrycznego. Tak działa wiele zabezpieczeń, np. SSL, TLS, IPsec. Więcej informacji dla szczególnie dociekliwych na stronach internetowych:
http://pl.wikipedia.org/wiki/Transport_Layer_Security
http://pl.wikipedia.org/wiki/IPsec).

W dużym uproszczeniu szyfrowanie SSL przebiega w następujący sposób:

- Serwer webowy ma certyfikat z kluczem publicznym oraz certyfikat z kluczem publicznym i prywatnym
- Przeglądarka internetowa łączy się do serwera webowego i prosi o zaszyfrowanie komunikacji
- Serwer przesyła przeglądarce klucz publiczny
- Przeglądarka tworzy losowo klucz symetryczny, zwany w tym przypadku kluczem sesji. Aby bezpiecznie przesłać klucz sesji do serwera, szyfruje go otrzymanym kluczem publicznym
- Wynik szyfrowania przesyła do serwera
- Serwer posiada klucz prywatny niezbędny do odszyfrowania klucza sesji

- Po bezpiecznej wymianie symetrycznego klucza sesji, dalsza komunikacja może być zabezpieczona symetrycznym kluczem sesji, znanym tylko przeglądarce i serwerowi. Przeglądarce, bo go wygenerowała, więc ma go przed zaszyfrowaniem, serwerowi WWW, ponieważ otrzymał zaszyfrowany klucz sesji jego kluczem publicznym, ale dzięki posiadaniu klucza prywatnego było możliwe jego odszyfrowanie.

Innym wykorzystaniem klucza publicznego i prywatnego jest podpis elektroniczny. W tym przypadku wykorzystywana jest tzw. funkcja skrótu, czyli mieszająca (hash). Funkcja mieszająca jest działaniem matematycznie nieodwracalnym (ale nie do końca ☹).

Wyobraźmy sobie sytuację, gdy chcemy potwierdzić, że obie strony znają to samo hasło, ale bez jego ujawniania. Przyjmijmy, że hasło jest dowolną liczbą. Skrót wykonamy w ten sposób, że dodamy do siebie wszystkie cyfry liczby, gdy liczba ma więcej niż 1 cyfrę, ponawiamy działanie. Następnie uzyskaną tak liczbę jednocyfrową mnożymy przez wartość klucza.

Przyjmijmy, że hasło to 19345. Ustalamy jawnie, że kluczem jest 3.

Jedna strona wykonuje działanie 1 + 9 + 3 + 4 + 5 = 22; 2 + 2 = 4,

wynik mnoży przez klucz 4 * 3 = 12

i 12 przesyła do drugiej strony.

Druga strona wykonuje takie samo działanie 1 + 9 + 3 + 4 + 5 = 22; 2 + 2 = 4,

wynik mnożymy przez klucz 4 * 3 = 12.

Czyli obie strony znają to samo hasło (albo hasło, które w wyniku działania daje ten sam wynik...).

Przyjmijmy, że każda ze stron zna inną wartość hasła.

Jedna myśli, że hasło to 12, a druga, że 1234.

Ustalają jawnie, że kluczem jest 2.

Pierwsza strona wykonuje działanie 1 + 2 = 3.

Wynik mnoży przez klucz 3 * 2 = 6,

czyli przesyła 06.

Druga strona wykonuje działanie 1 + 2 + 3 + 4 = 10, 1 + 0 = 1.

Wynik mnoży przez klucz 1 * 2 = 2.

Porównuje otrzymane 06 z obliczonym 02.

Wartości są różne, więc hasła są niezgodne.

Ale przy tak prostym algorytmie, różne hasła mogą dać taki sam wynik:

Na przykład pierwsza strona z hasłem 12 i kluczem 2 uzyskała wynik 06.

Gdyby druga strona uważała, że hasło to 1245, to przy kluczu 2

wykonuje działanie: 1 + 2 + 4 + 5 = 12, 1 + 2 = 3,

wynik mnoży przez klucz 3 + 2 = 6.

Porównuje otrzymany wynik 06 z obliczonym wynikiem 06 i uznaje błędnie, że obie strony znają to samo hasło.

Dlatego stosuje się algorytmy, przy których uzyskanie z różnych wartości wejściowych takiego samego wyniku jest bardzo mało prawdopodobne. W ubiegłym wieku najbardziej znane były algorytmy: MD5 i SHA-1 (obecnie uznawane za słabe). Więcej informacji podają strony internetowe o adresach: http://pl.wikipedia.org/wiki/MD5 oraz http://pl.wikipedia.org/wiki/SHA-1.

Za bezpieczny uznaje się algorytm SHA-2 (więcej na stronie internetowej: http://pl.wikipedia.org/wiki/SHA-2), natomiast w roku 2012 opracowano SHA-3 (więcej na stronie: http://pl.wikipedia.org/wiki/SHA-3).

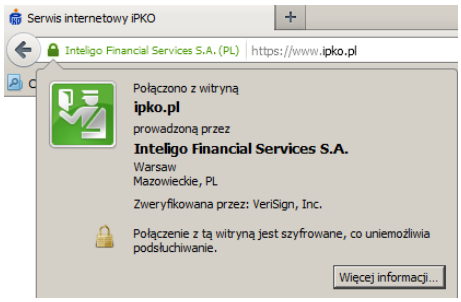
Funkcja mieszająca może być użyta jako suma kontrolna sprawdzająca, czy dokument nie uległ zmianie. Do opracowanego dokumentu dodaje się jego sumę kontrolną. Jeśli dokument uległ zmianie (uszkodzeniu), to suma kontrolna będzie miała inną wartość. Gdy do utworzenia sumy kontrolnej użyjemy pary kluczy asymetrycznych, mamy podpis elektroniczny. W celu wygenerowania sumy kontrolnej używa się klucza prywatnego. Klucz publiczny nie pozwala na wygenerowanie podpisu, ale umożliwia sprawdzenie, czy dokument nie uległ zmianie oraz czy został podpisany przez odpowiadający kluczowi publicznemu klucz prywatny. Więcej informacji podają strony:
http://pl.wikipedia.org/wiki/Funkcja_skr%C3%B3tu,
http://pl.wikipedia.org/wiki/Hash.

Jak wspomniano, para kluczy prywatny i publiczny jest opakowana w certyfikat, który wystawia urząd autoryzacji (Certification Authority, CA). Mechanizm oparty jest na zaufaniu do CA. Zakładamy, że wystawiając nam certyfikat z parą kluczy prywatny i publiczny, urząd nigdy nikomu (poza nami) nie ujawni naszego klucza prywatnego. Na podobnej zasadzie działają dokumenty tożsamości.

Przyjmujemy, że gdy otrzymujemy dokument tożsamości (np. dowód osobisty) urząd nikomu obcemu nie wystawi „kopii" naszego dokumentu tożsamości. Notabene, na zaufaniu opiera się system bankowy. Gdy na nasze konto wpływają środki, wierzymy, że nikt nieupoważniony nie będzie miał do nich dostępu. Złamanie takiego zaufania może spowodować tzw. syndrom cypryjski – klienci nie będą powierzali swoich środków danemu systemowi bankowemu, w sytuacji gdy stracą pewność ich bezpieczeństwa.

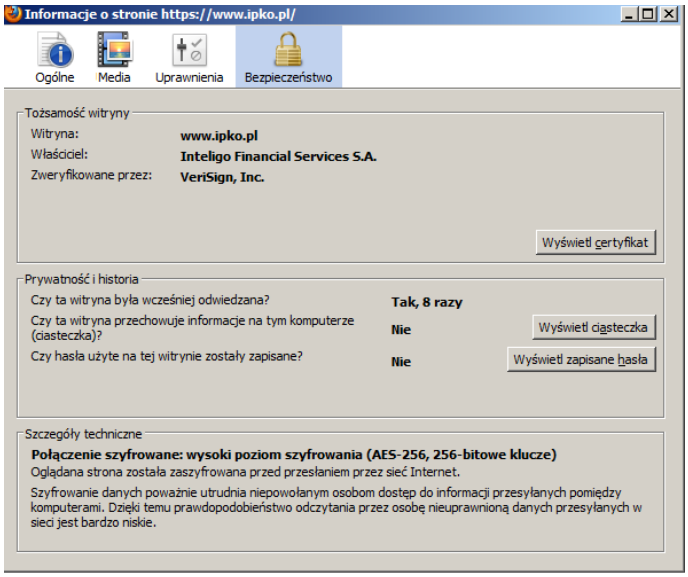
Ufamy pewnej grupie instytucji finansowych, cieszących się powszechnym zaufaniem, dodatkowo popartym zewnętrznymi gwarancjami, a innym po prostu nie.

Wracając do CA i certyfikatu wystawionego dla serwera np. WWW – oprócz pary kluczy: publicznego i prywatnego certyfikat zawiera wiele dodatkowych informacji. Gdy łączymy się do witryny zabezpieczonej SSL, używamy protokołu HTTPS (np. witryna banku PKO BP).



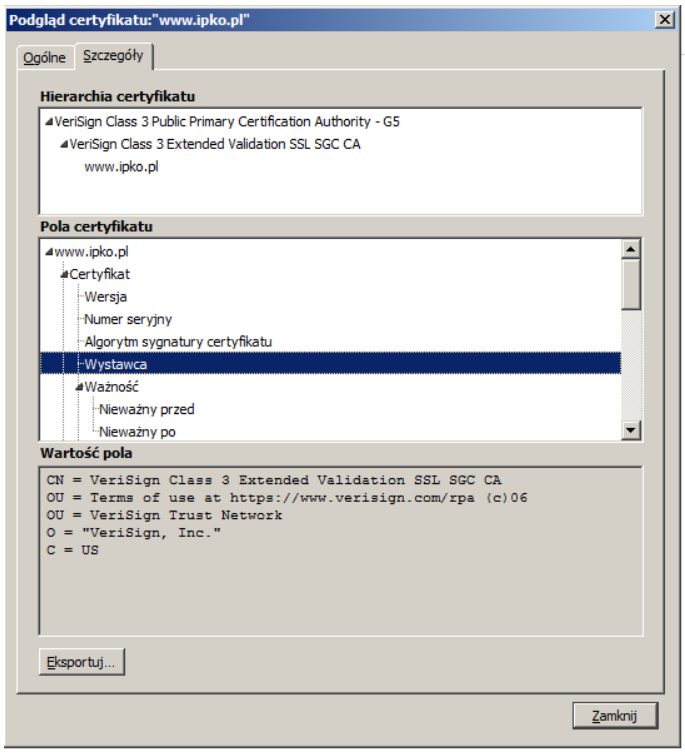
Rysunek 1. Połączenie HTTPS do ipko.pl banku PKOBP

Ikona kłódki oznacza bezpieczne połączenie. Klikając możemy zobaczyć informacje o certyfikacie, a gdy klikniemy na przycisk **Więcej informacji...**



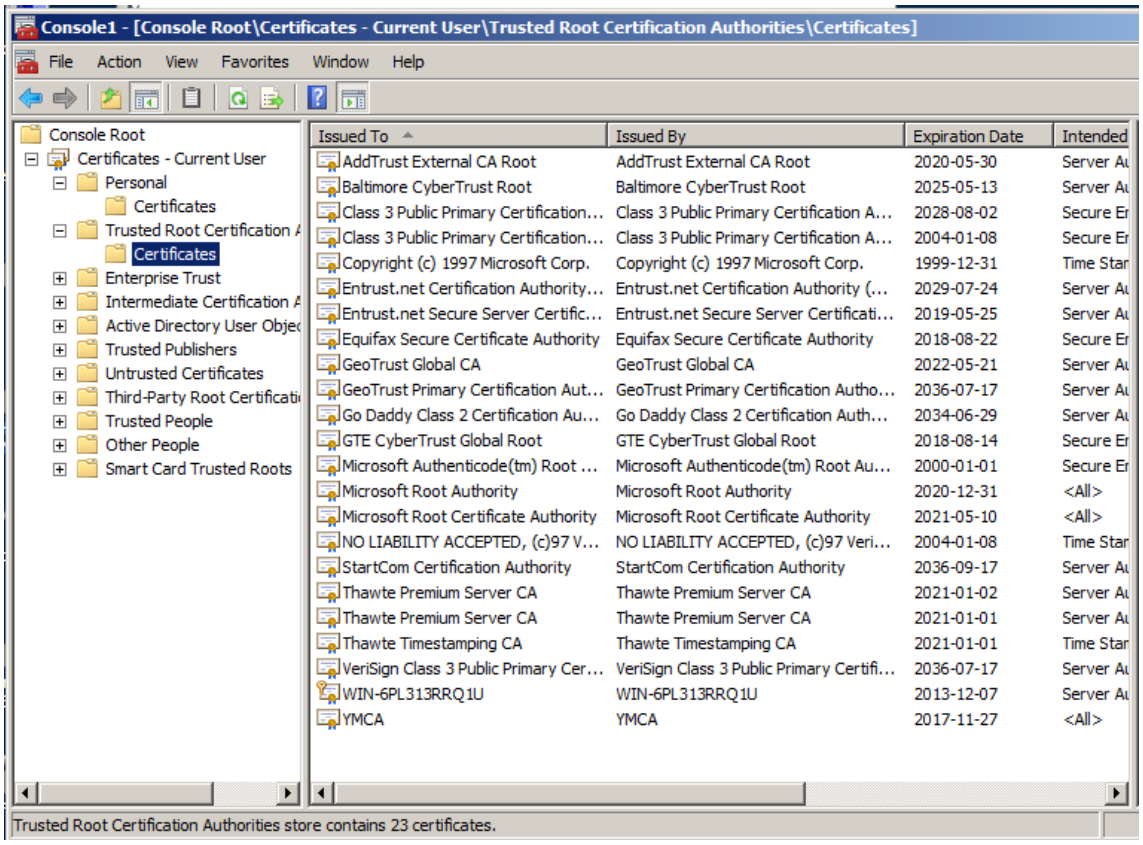
Rysunek 2. Informacje o certyfikacie witryny www.ipko.pl

a następnie **Wyświetl certyfikat,** możemy uzyskać o nim wszystkie informacje poza kluczem prywatnym w nim zawarte.



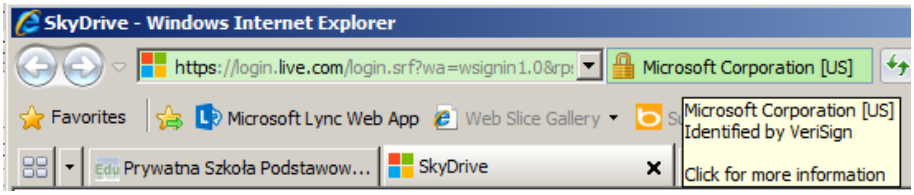
Rysunek 3. Szczegóły certyfikatu witryny www.ipko.pl

Wiemy, między innymi, kto wystawił certyfikat. Jest także lista domyślnie zaufanych wystawców certyfikatów, którą możemy sprawdzić na swoim komputerze w przystawce certyfikaty w narzędziu MMC.



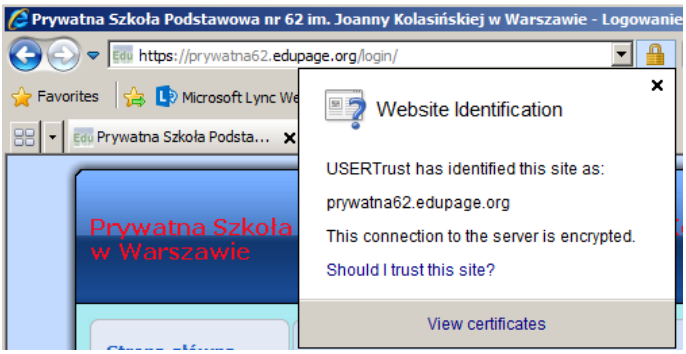
Rysunek 4. Lista domyślnie zaufanych CA

Przy otwieraniu witryny należy zwrócić uwagę na kolor paska adresu i certyfikatu. Kolor zielony oznacza, że certyfikat został poddany rygorystycznym procedurom weryfikacji.



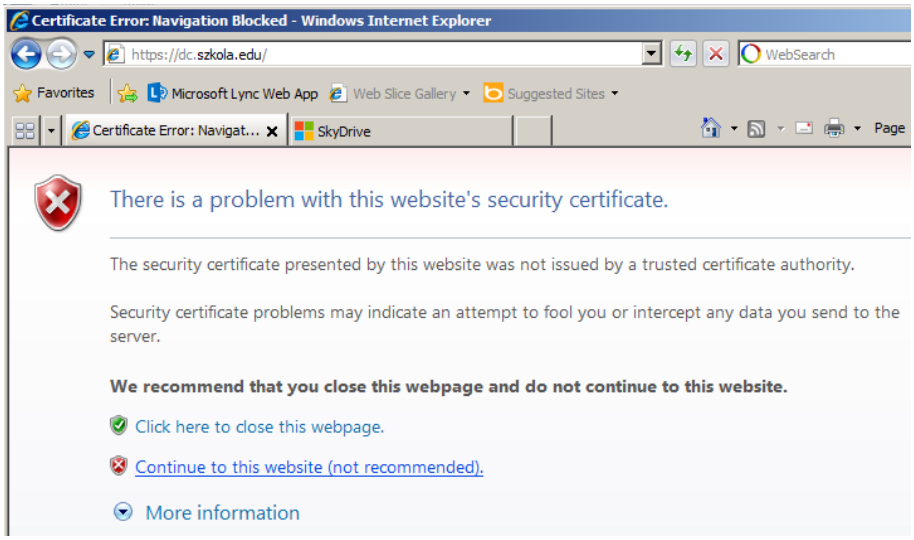
Rysunek 5. Witryna firmy Microsoft poddana rygorystycznej weryfikacji

Kolor niebieski certyfikatu oznacza zabezpieczenie witryny zwykłym certyfikatem. Jest on prawidłowy, ale nie został poddany kosztownej procedurze weryfikacji.



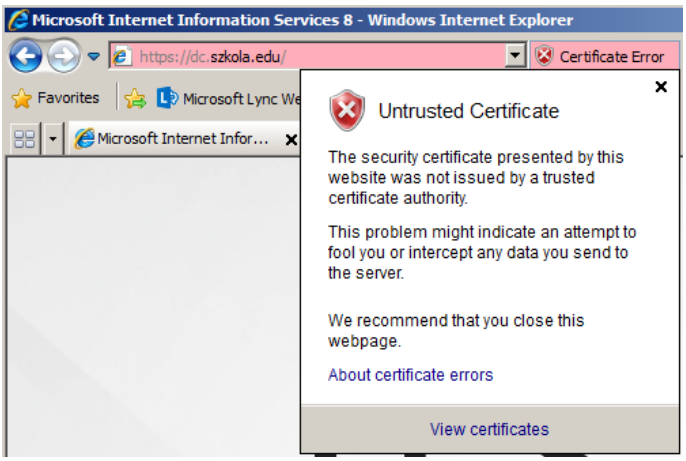
Rysunek 6. Witryna zabezpieczona zwykłym certyfikatem

Kolor czerwony oznacza nieprawidłowości certyfikatu.



Rysunek 7. Błąd certyfikatu

Pomimo to możemy podjąć ryzyko otwarcia witryny, wciskając link



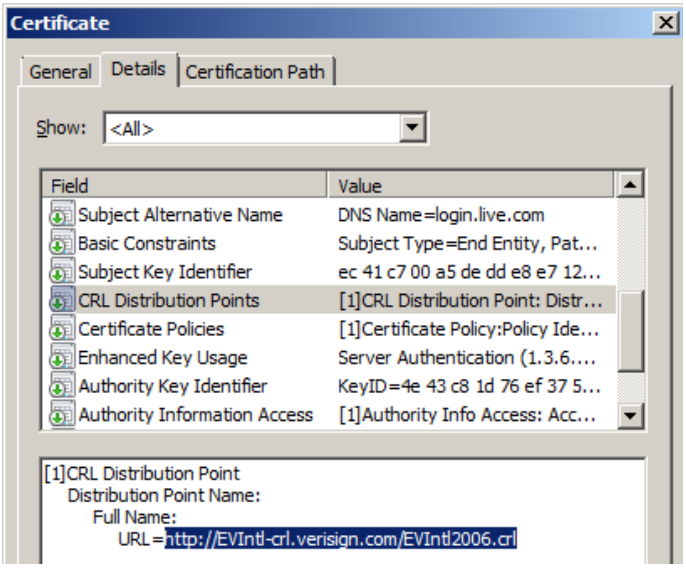
Rysunek 8. Błąd certyfikatu – niepewne centrum autoryzacji CA

Najczęstsze błędy certyfikatu to:

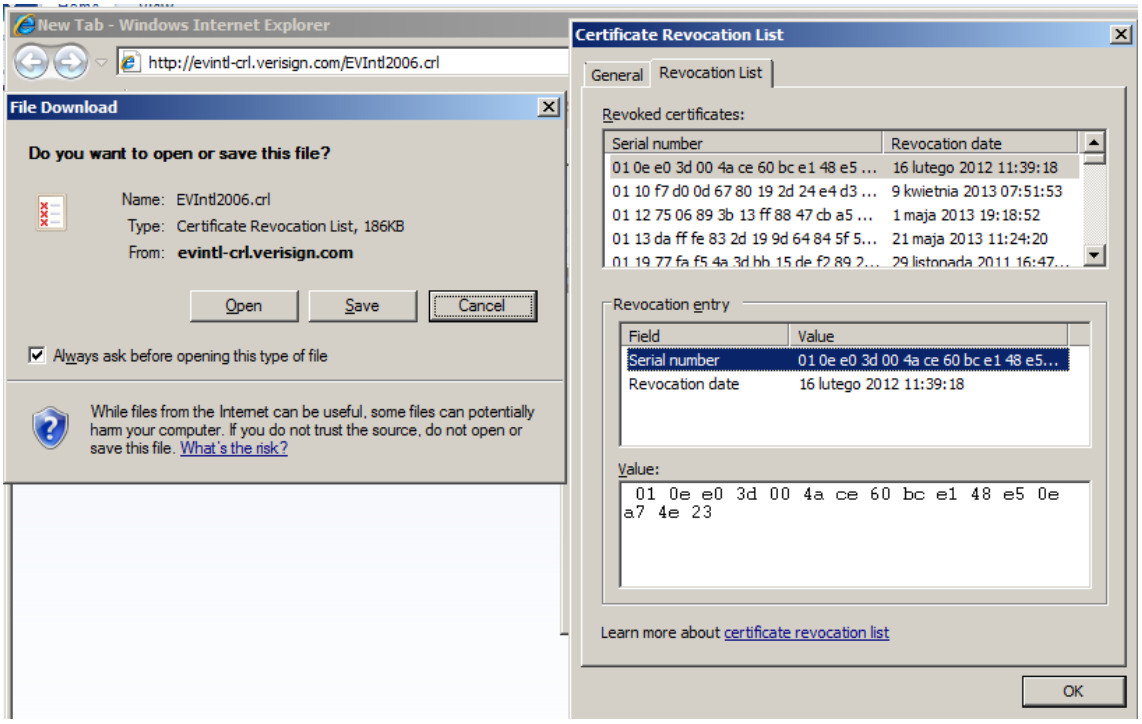
- Certyfikat zabezpieczeń tej witryny nie pochodzi z zaufanego źródła – właściciel witryny najprawdopodobniej skorzystał z własnego CA, nie chcąc płacić za certyfikat godny zaufania.
- Certyfikat zabezpieczeń tej witryny jest nieaktualny – certyfikat jest przydzielany na określony czas, administrator nie przedłużył ważności. Inną przyczyną może być przestawiony zegar czasu w Twoim komputerze.
- Adres tej witryny nie odpowiada adresowi zawartemu w certyfikacie zabezpieczeń – nazwa witryny jest inna niż zapisana w certyfikacie.
- Certyfikat zabezpieczeń tej witryny został odwołany – odwołanie, unieważnienie certyfikatu jest wykonywane zazwyczaj w sytuacji kompromitacji certyfikatu np. kradzieży klucza prywatnego.

Unieważnienie certyfikatu jest działaniem drastycznym. Polega ono na opublikowaniu numeru seryjnego (*serial number*) unieważnionego certyfikatu na liście **CRL** (*Certificate Revocation List*, czyli lista unieważnionych certyfikatów). Działanie to jest trochę podobne do zgłoszenia zagubienia lub kradzieży dowodu tożsamości.

Każdy certyfikat ma zapisany adres **CRL,** gdzie można sprawdzić, czy nie został on unieważniony.



Rysunek 9. Adres CRL w certyfikacie



Rysunek 10. CRL – lista unieważnionych certyfikatów

Programy, w tym przeglądarki internetowe, zazwyczaj automatycznie sprawdzają, czy certyfikat nie został unieważniony i opublikowany na liście CRL.

Komunikacja pomiędzy usługami serwera a klientem może być zabezpieczona za pomocą SSL, co jest bardzo wygodnym rozwiązaniem, ale każda usługa musi być niezależnie do tego ustawiona. Niektóre usługi nie mają wsparcia dla szyfrowania SSL. Można w takiej sytuacji zaszyfrować cały ruch na serwerze za pomocą protokołu IPSec

(bezpieczne IP) lub za pomocą VPN (*Virtual Private Network*, rodzaj wirtualnego kabla, tunelu, łączącego dwa oddziały firmy lub komputer pracownika z firmą).

W niektórych sytuacjach użycie VPN jest konieczne również z innego powodu. Adresy IP (podobnie jak numery telefonów) zostały podzielone na adresy prywatne – działające tylko w obrębie firmy (tak jak numery wewnętrzne telefonów) oraz na adresy IP publiczne – działające w Internecie (tak jak publiczne numery telefonów).

Analogiczna jest tutaj konfiguracja, gdy z telefonów wewnętrznych można dzwonić na zewnętrzne, ale z zewnątrz nie można dodzwonić się do numeru wewnętrznego. Można wtedy dodać wybranym numerom publicznym przypisania przekierowania rozmowy na numer wewnętrzny, jeśli to nie zostanie zrobione, nie można dzwonić z zewnątrz na numery wewnętrzne. Jedną z przyczyn jest to, że numery wewnętrzne telefonów w wielu firmach będą się powtarzać.

Podobnie jest w przypadku adresów prywatnych IP. Natomiast użycie VPN działa jak położenie wirtualnego kabla telefonicznego pomiędzy firmami, które ustaliły przydział wewnętrznych numerów telefonów. Pracownicy tych firm nie muszą używać telefonów publicznych do rozmów między sobą, wystarczą numery prywatne. Samo użycie VPN pozwala na komunikację pomiędzy prywatnymi numerami IP, ale nie zawsze gwarantuje silne zabezpieczenie „kabla – tunelu komunikacyjnego". Szyfrowanie i podpisywanie przesyłanych danych jest dodatkową funkcjonalnością VPN.

Oprócz zabezpieczenia samego kanału komunikacji, należy pamiętać, że łącząc się do wybranego serwera możemy zarazić nasz komputer różnymi szkodliwymi programami. W Microsoft Windows Vista i nowszych wprowadzono dodatkowe mechanizmy ostrzegawcze, które przy działaniach przypuszczalnie niebezpiecznych ostrzegają nas przed POTENCJALNYM zagrożeniem. To trochę tak jak ostrzeganie dziecka: „Nie dotykaj, nie bierz do buzi, najpierw pokaż, zobaczę co to jest" przy każdej czynności dziecka. Jest co prawda bardzo uciążliwe, ale zwraca uwagę, w sytuacjach gdy wzrasta ryzyko zagrożeń. Łącząc się do istotnych serwerów zabezpieczonych certyfikatem, należy dokładnie go zweryfikować. Istnieje ryzyko, że ktoś utworzył certyfikat bardzo podobny np. do certyfikatu banku. Certyfikaty mogą różnić się np. jednym znakiem w nazwie... Podobnie jak dobrze podrobiony banknot trudno odróżnić od prawdziwego.

Odrębna grupa to certyfikaty wystawione przez mało znane (lub wewnątrzfirmowe) serwery CA. Samodzielnie musimy podjąć decyzję, czy ufamy takiemu CA (podobnie jak osobie znajomej, która obiecuje, że odda pożyczone pieniądze).

Jedną z niezwykle użytecznych funkcji, jakie dają nam nowe technologie jest **podpis elektroniczny**. Może on zostać wykorzystany do podpisywania wiadomości e-mail, dokumentów czy innych plików. Do wykonania podpisu elektronicznego potrzebny jest odpowiedni certyfikat, a korzystanie z niego w Polce reguluje ustawa z dnia 18 września 2001 r. o podpisie elektronicznym: http://isap.sejm.gov.pl/Download?id=WDU20011301450&type=2

Certyfikat kwalifikowany jest to podpis, który w myśl polskiej ustawy o podpisie elektronicznym posiada status równoważny z własnoręcznym podpisem. Certyfikaty kwalifikowane w Polsce wydają:

- UNIZETO TECHNOLOGIES
- POLSKA WYTWÓRNIA PAPIERÓW WARTOŚCIOWYCH
- TP INTERNET
- KRAJOWA IZBA ROZLICZENIOWA

Zamiast kosztownego podpisu kwalifikowanego w większości przypadków można użyć podpisu niekwalifikowanego, który często można uzyskać bezpłatnie, np. z witryny: https://www.comodo.com/home/email-security/free-email-certificate.php.

Za pomocą takiej parafki można podpisywać pocztę, co pozwala sprawdzić wiarygodność nadawcy, zagwarantować, że dane nie uległy zmianie. Do podpisywania używa się klucza prywatnego. Powszechnie dostępny klucz publiczny pozwala na zweryfikowanie autentyczności podpisu. Klucz publiczny stosujemy do kodowania wiadomości przesyłanej do odbiorcy posiadającego klucz prywatny, który jest niezbędny do odszyfrowania poczty.