WorkshopIT

Komputer narzędziem w rękach prawnika

Krzysztof Kamiński,
Sąd Okręgowy we Wrocławiu,
Wrocław, 16 listopada 2006r.

Agenda

- Bezpieczeństwo przepływu informacji w systemach informatycznych
  - Hasła i inne sposoby uwierzytelniania
  - Infrastruktura kluczy publicznych
  - Sposoby bezpiecznego logowania na stronach WWW
  - Bezpieczeństwo poczty elektronicznej
  - Komunikatory internetowe a możliwość podsłuchu
  - Bezpieczeństwo systemu operacyjnego
  - Zabezpieczenie danych na nośnikach typu PenDrive

Dlaczego zabezpieczać dane?

- Digitalizacja danych poufnych
- Wymiana informacji z klientem w formie elektronicznej
- Odpowiedzialność za ujawnienia informacji poufnych
- Dostęp do kont bankowych
- Szpiegostwo gospodarcze

Uwierzytelnianie

- Udowodnienie tożsamości
  - Użytkownika względem serwera (komputera)
  - Serwera względem użytkownika

Uwierzytelnianie / Scenariusz 1

- Login / Hasło - Nazwa Serwera
  - Serwer uwierzytelniony przez nazwę DNS przetłumaczoną na adres IP
  - Użytkownik uwierzytelniony przez login i hasło

Funkcja skrótu (hash)

- Przechowywanie jedynie skrótów haseł

Silne hasła

- Zabezpieczone przed prostymi metodami łamania haseł: słownikową, bruteforce, inkrementacyjną.
- Jeden z algorytmów tworzenia silnego hasła:
  - Wybranie łatwego do zapamiętania zdania
    - Nie ma lepszego wydziału niż Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.
  - Utworzyć skrót z pierwszych liter wszystkich wyrazów w powyższym zdaniu:

NmlwnWPAiEUW

Silne hasła, c.d.

NmlwnWPAiEUW

- Zastąpić wg znanego sobie wzoru np. l=!, W=# kilka liter w haśle

Nm!wn#PAiEU#

- Jeśli hasło ma być często zmieniane warto w środek dodać np. datę zmiany z wciśniętym klawiszem SHIFT np. 16/11 = !^?!!

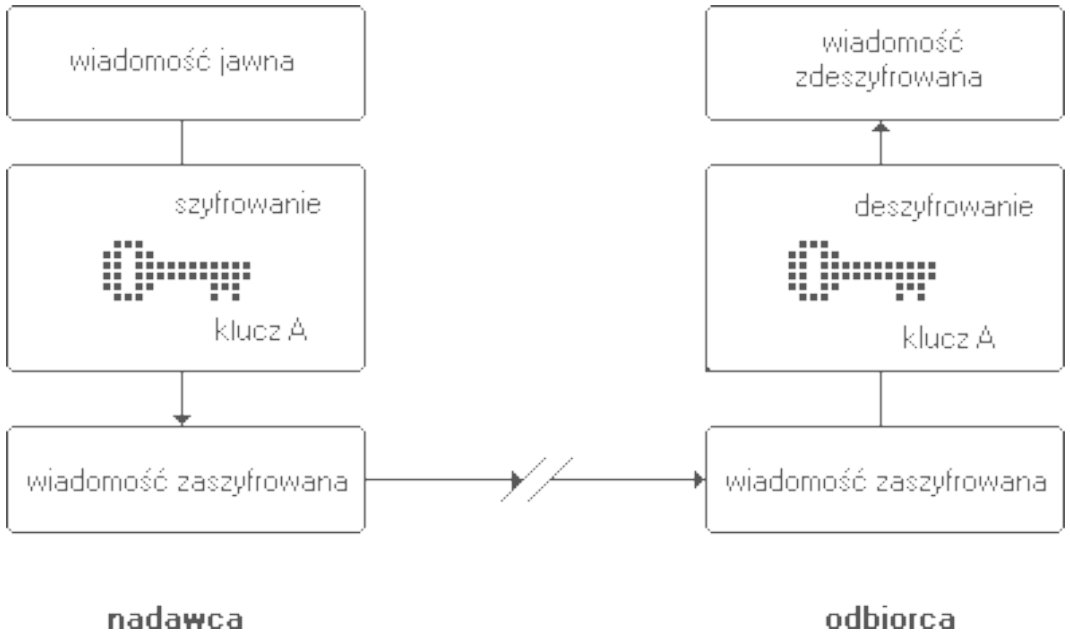
Nm!wn#!^?!!PAiEU#

Biometryczne metody uwierzytelniania

- Odcisk palca
- Kształt dłoni
- Wzór tęczówki oka
- Dynamika pisania na klawiaturze
- Sposób chodzenia
- Układ naczyń krwionośnych twarzy (mapa temp.)
- Dynamika ruchu gałek ocznych

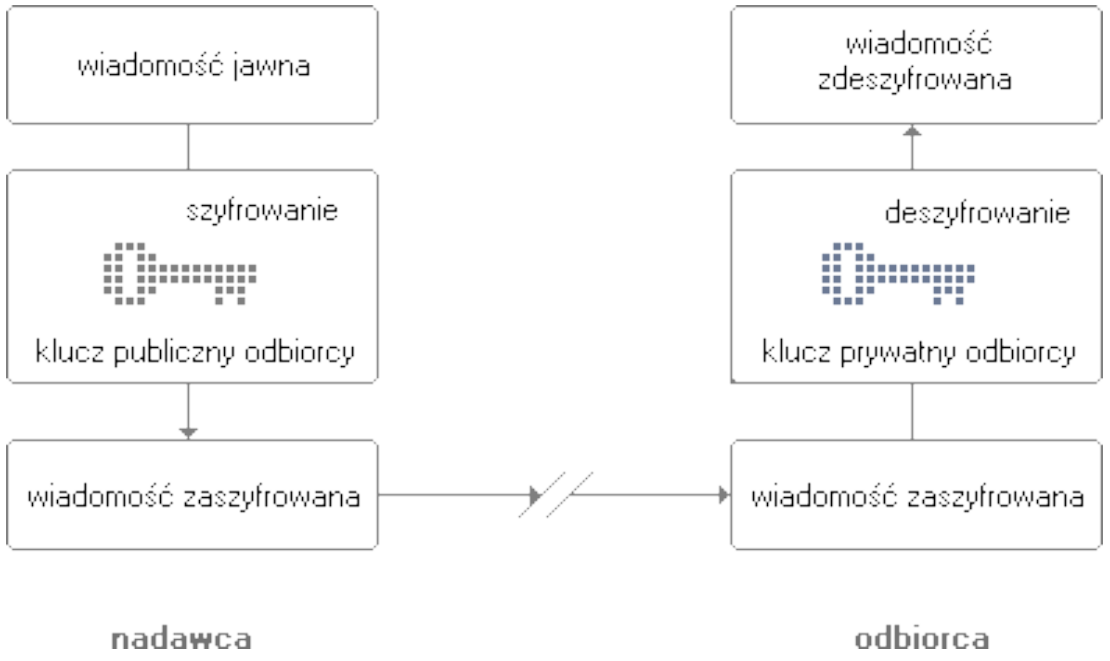
Infrastruktura Kluczy Publicznych

- Szyfrowanie symetryczne



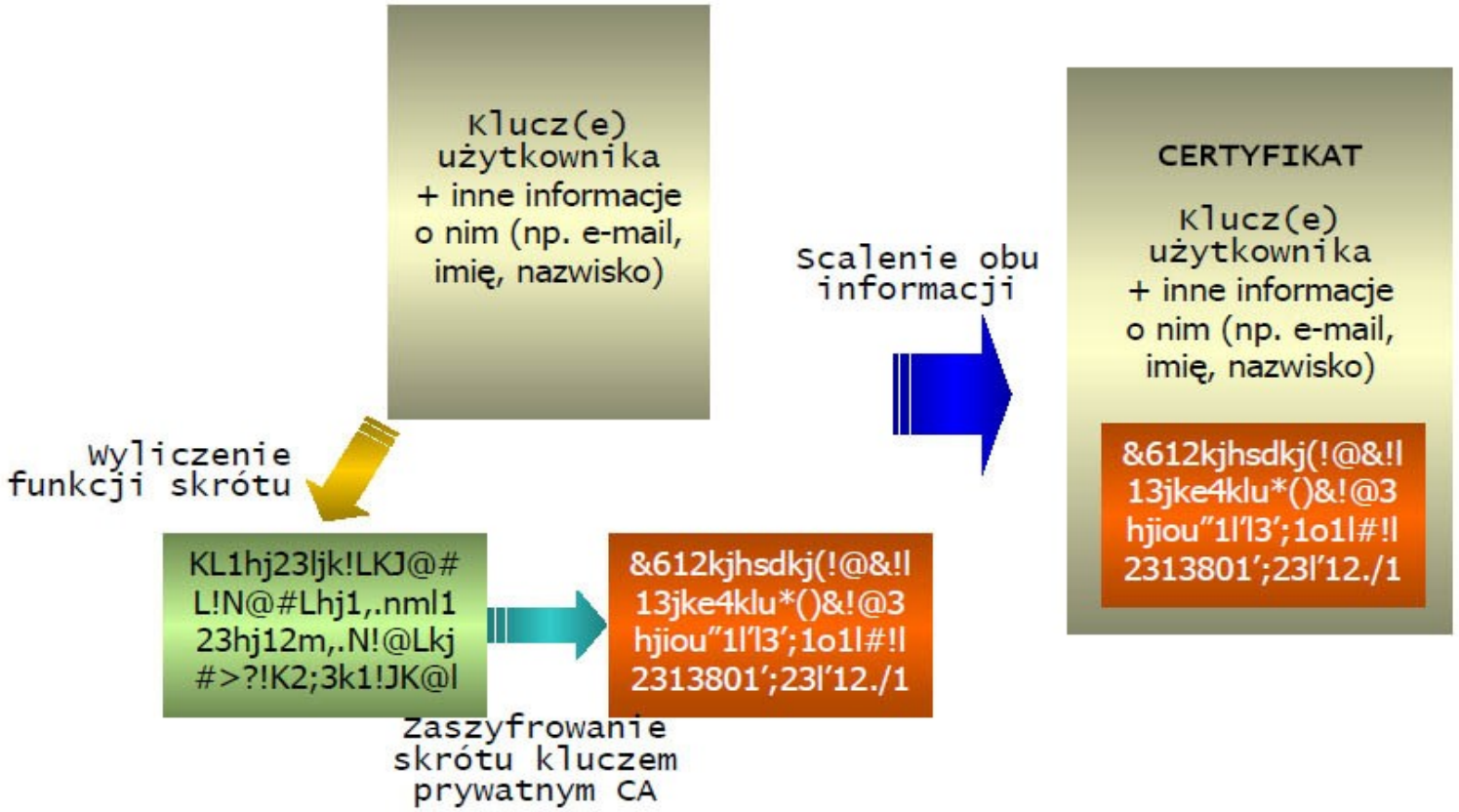
Infrastruktura Kluczy Publicznych

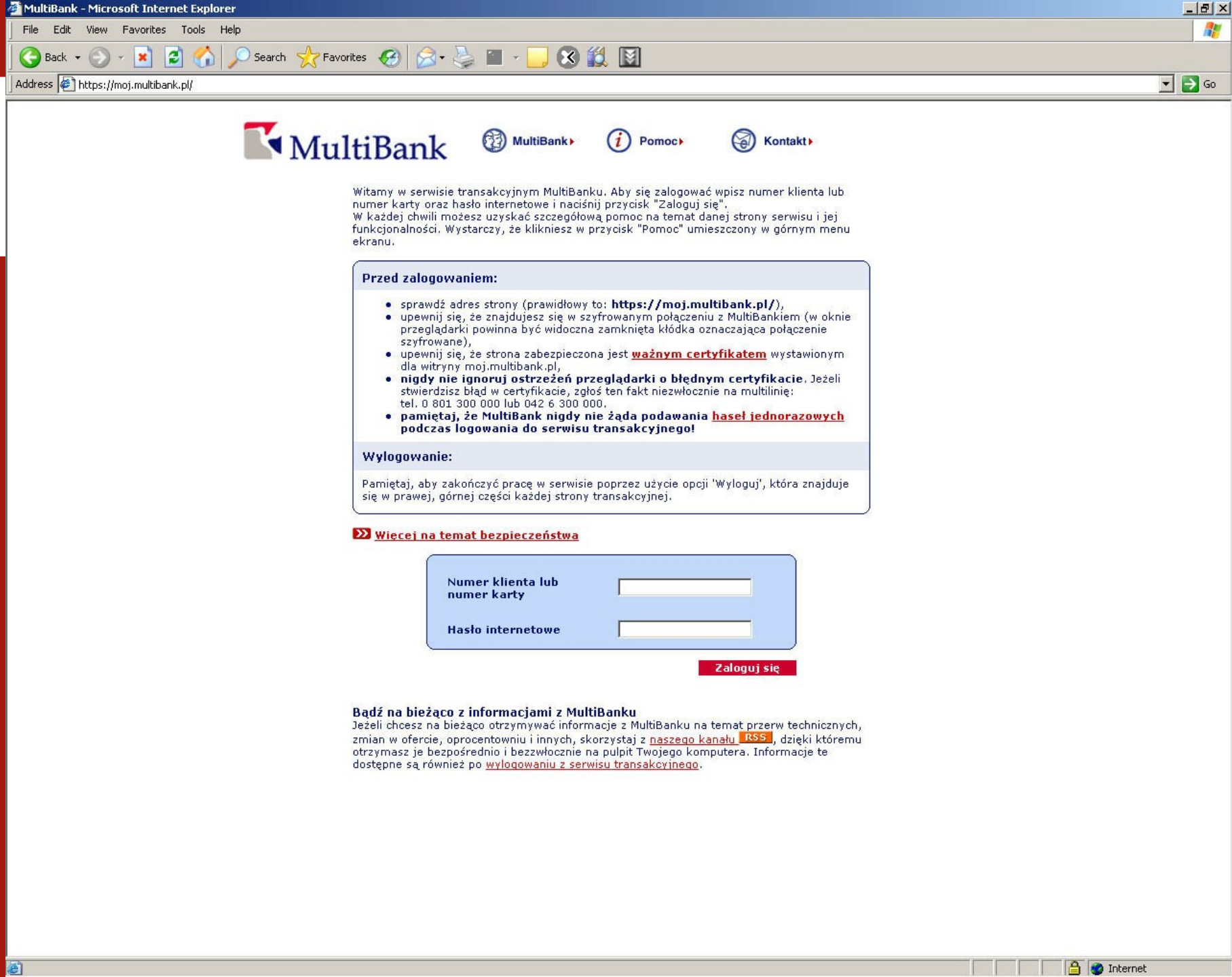
- Szyfrowanie asymetryczne



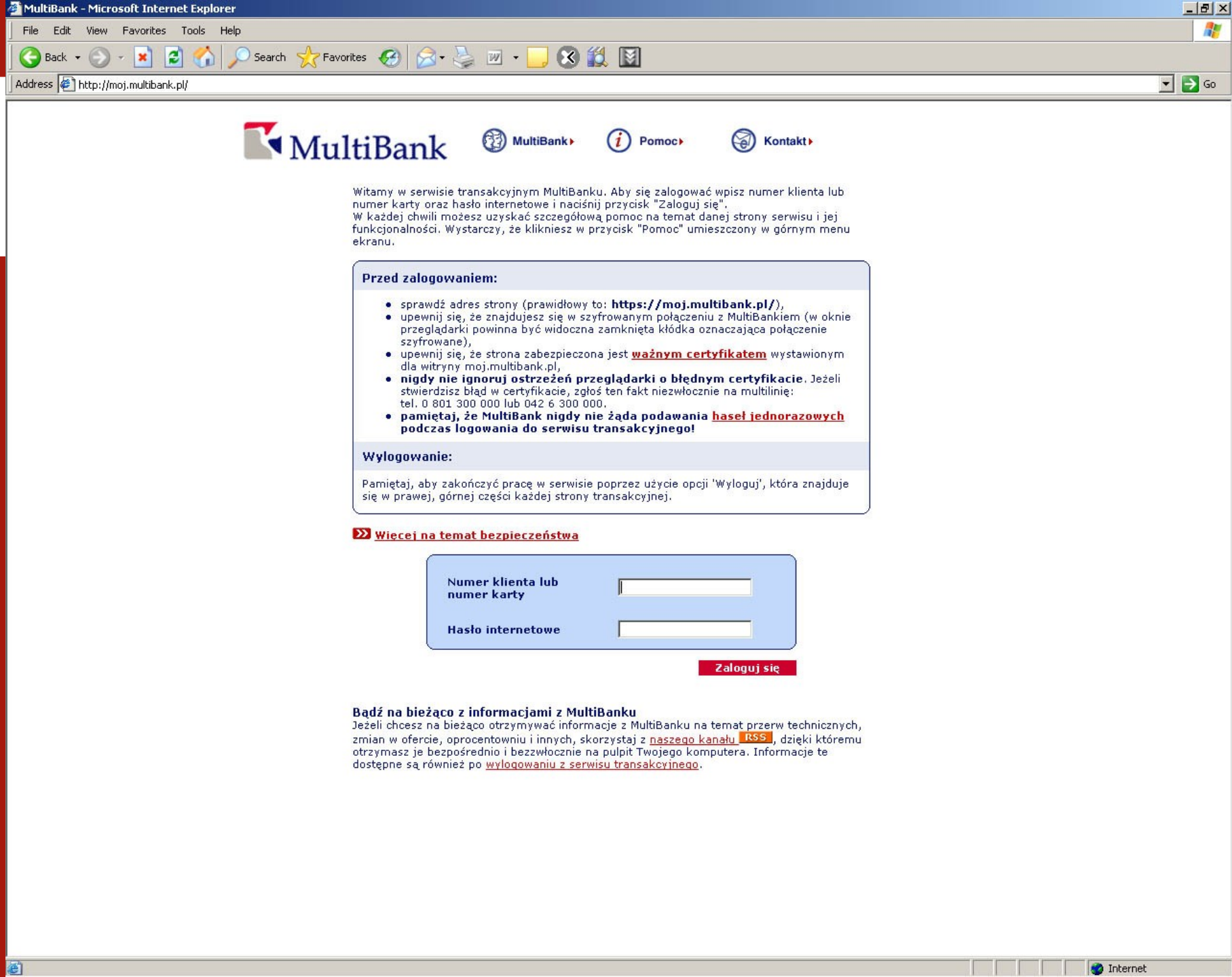
Infrastruktura Kluczy Publicznych

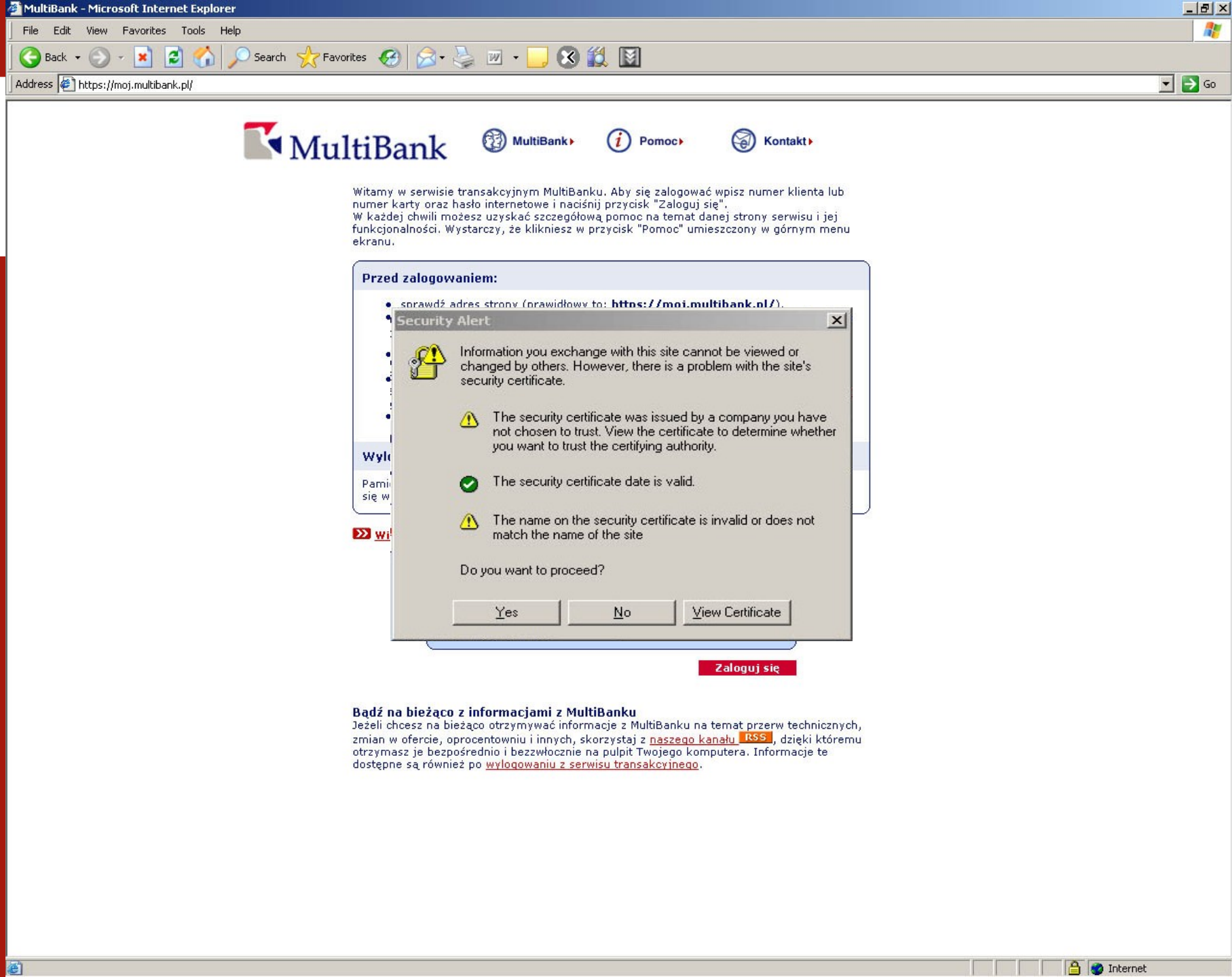
- Certyfikat cyfrowy




MultiBank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://moj.multibank.pl/
Go
MultiBank
MultiBank
Pomoc
Kontakt
Witamy w serwisie transakcyjnym MultiBanku. Aby się zalogować wpisz numer klienta lub numer karty oraz hasło internetowe i naciśnij przycisk "Zaloguj się".
W każdej chwili możesz uzyskać szczegółową pomoc na temat danej strony serwisu i jej funkcjonalności. Wystarczy, że klikniesz w przycisk "Pomoc" umieszczony w górnym menu ekranu.
Przed zalogowaniem:
sprawdź adres strony (prawidłowy to: https://moj.multibank.pl/),
upewnij się, że znajdujesz się w szyfrowanym połączeniu z MultiBankiem (w oknie przeglądarki powinna być widoczna zamknięta kłódka oznaczająca połączenie szyfrowane),
upewnij się, że strona zabezpieczona jest ważnym certyfikatem wystawionym dla witryny moj.multibank.pl,
nigdy nie ignoruj ostrzeżeń przeglądarki o błędnym certyfikacie. Jeżeli stwierdzisz błąd w certyfikacie, zgłoś ten fakt niezwłocznie na multilinię: tel. 0 801 300 000 lub 042 6 300 000.
pamiętaj, że MultiBank nigdy nie żąda podawania haseł jednorazowych podczas logowania do serwisu transakcyjnego!
Wylogowanie:
Pamiętaj, aby zakończyć pracę w serwisie poprzez użycie opcji 'Wyloguj', która znajduje się w prawej, górnej części każdej strony transakcyjnej.
Więcej na temat bezpieczeństwa
Numer klienta lub numer karty
Hasło internetowe
Zaloguj się
Bądź na bieżąco z informacjami z MultiBanku
Jeżeli chcesz na bieżąco otrzymywać informacje z MultiBanku na temat przerw technicznych, zmian w ofercie, oprocentowniu i innych, skorzystaj z naszego kanału RSS, dzięki któremu otrzymasz je bezpośrednio i bezzwłocznie na pulpit Twojego komputera. Informacje te dostępne są również po wylogowaniu z serwisu transakcyjnego.
Internet

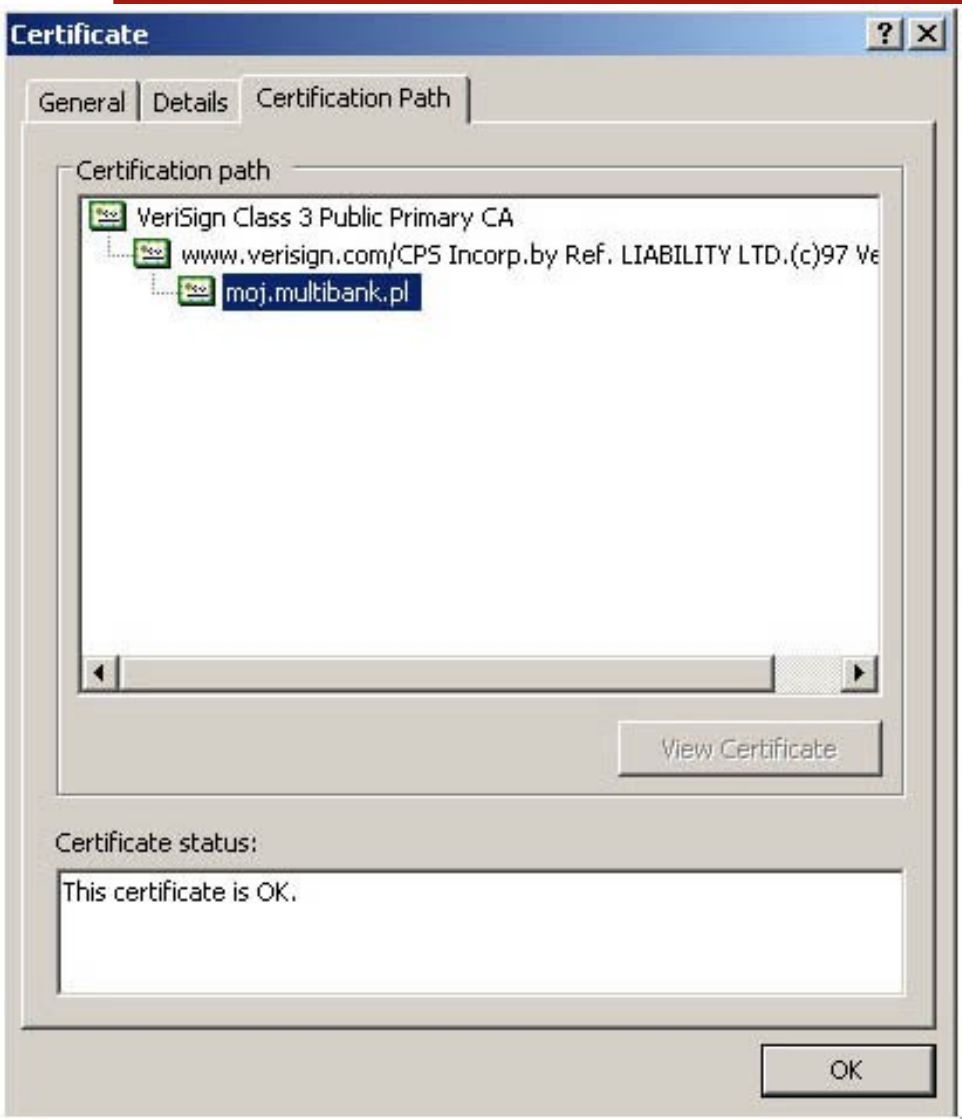

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
•Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: moj.multibank.pl
Issued by: www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
Valid from 2006-04-26 to 2007-06-16
Install Certificate...
Issuer Statement
OK

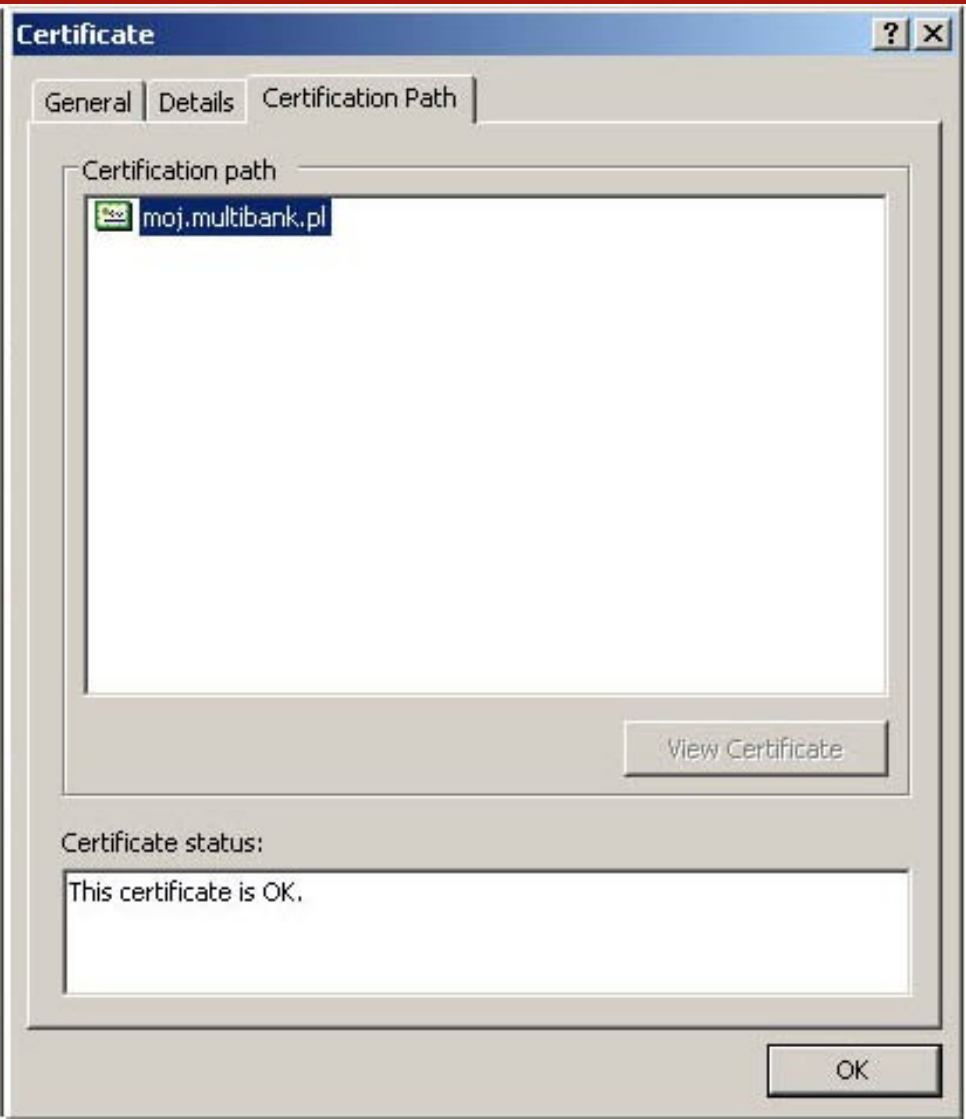

MultiBank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://moj.multibank.pl/
Go
MultiBank
MultiBank
Pomoc
Kontakt
Witamy w serwisie transakcyjnym MultiBanku. Aby się zalogować wpisz numer klienta lub numer karty oraz hasło internetowe i naciśnij przycisk "Zaloguj się".
W każdej chwili możesz uzyskać szczegółową pomoc na temat danej strony serwisu i jej funkcjonalności. Wystarczy, że klikniesz w przycisk "Pomoc" umieszczony w górnym menu ekranu.
Przed zalogowaniem:
sprawdź adres strony (prawidłowy to: https://moj.multibank.pl/),
upewnij się, że znajdujesz się w szyfrowanym połączeniu z MultiBankiem (w oknie przeglądarki powinna być widoczna zamknięta kłódka oznaczająca połączenie szyfrowane),
upewnij się, że strona zabezpieczona jest ważnym certyfikatem wystawionym dla witryny moj.multibank.pl,
nigdy nie ignoruj ostrzeżeń przeglądarki o błędnym certyfikacie. Jeżeli stwierdzisz błąd w certyfikacie, zgłoś ten fakt niezwłocznie na multilinię: tel. 0 801 300 000 lub 042 6 300 000.
pamiętaj, że MultiBank nigdy nie żąda podawania haseł jednorazowych podczas logowania do serwisu transakcyjnego!
Wylogowanie:
Pamiętaj, aby zakończyć pracę w serwisie poprzez użycie opcji 'Wyloguj', która znajduje się w prawej, górnej części każdej strony transakcyjnej.
Więcej na temat bezpieczeństwa
Numer klienta lub numer karty
Hasło internetowe
Zaloguj się
Bądź na bieżąco z informacjami z MultiBanku
Jeżeli chcesz na bieżąco otrzymywać informacje z MultiBanku na temat przerw technicznych, zmian w ofercie, oprocentowniu i innych, skorzystaj z naszego kanału RSS, dzięki któremu otrzymasz je bezpośrednio i bezzwłocznie na pulpit Twojego komputera. Informacje te dostępne są również po wylogowaniu z serwisu transakcyjnego.
Internet


MultiBank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://moj.multibank.pl/
Go
MultiBank
MultiBank
Pomoc
Kontakt
Witamy w serwisie transakcyjnym MultiBanku. Aby się zalogować wpisz numer klienta lub numer karty oraz hasło internetowe i naciśnij przycisk "Zaloguj się".
W każdej chwili możesz uzyskać szczegółową pomoc na temat danej strony serwisu i jej funkcjonalności. Wystarczy, że klikniesz w przycisk "Pomoc" umieszczony w górnym menu ekranu.
Przed zalogowaniem:
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate
Zaloguj się
Bądź na bieżąco z informacjami z MultiBanku
Jeżeli chcesz na bieżąco otrzymywać informacje z MultiBanku na temat przerw technicznych, zmian w ofercie, oprocentowniu i innych, skorzystaj z naszego kanału RSS, dzięki któremu otrzymasz je bezpośrednio i bezzwłocznie na pulpit Twojego komputera. Informacje te dostępne są również po wylogowaniu z serwisu transakcyjnego.
Internet


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
•Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: moj.multibank.pl
Issued by: www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
Valid from 2006-04-26 to 2007-06-16
Install Certificate...
Issuer Statement
OK


Certificate
General
Details
Certification Path
Certificate Information
This certificate cannot be verified up to a trusted certification authority.
Issued to: moj.multibank.pl
Issued by: www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
Valid from 2006-11-15 to 2016-11-12
Install Certificate...
Issuer Statement
OK

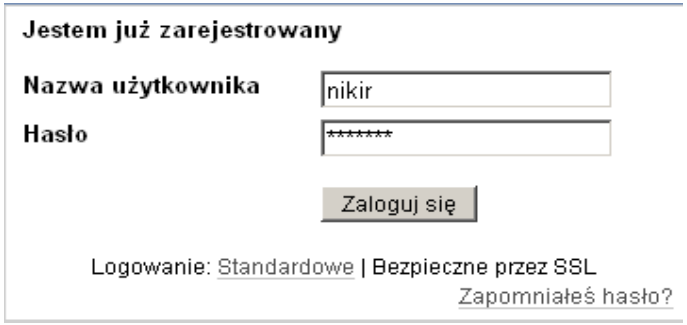

Certificate
General
Details
Certification Path
Certification path
VeriSign Class 3 Public Primary CA
www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 Ve
moj.multibank.pl
View Certificate
Certificate status:
This certificate is OK.
OK


Certificate
General
Details
Certification Path
Certification path
moj.multibank.pl
View Certificate
Certificate status:
This certificate is OK.
OK

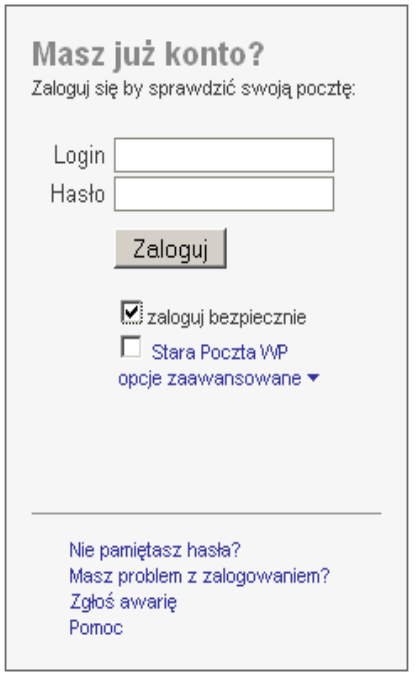
Sposoby bezpiecznego logowania na stronach WWW

- Bezwzględnie korzystać z formularzy bezpiecznego logowania

allegro.pl



poczta.wp.pl

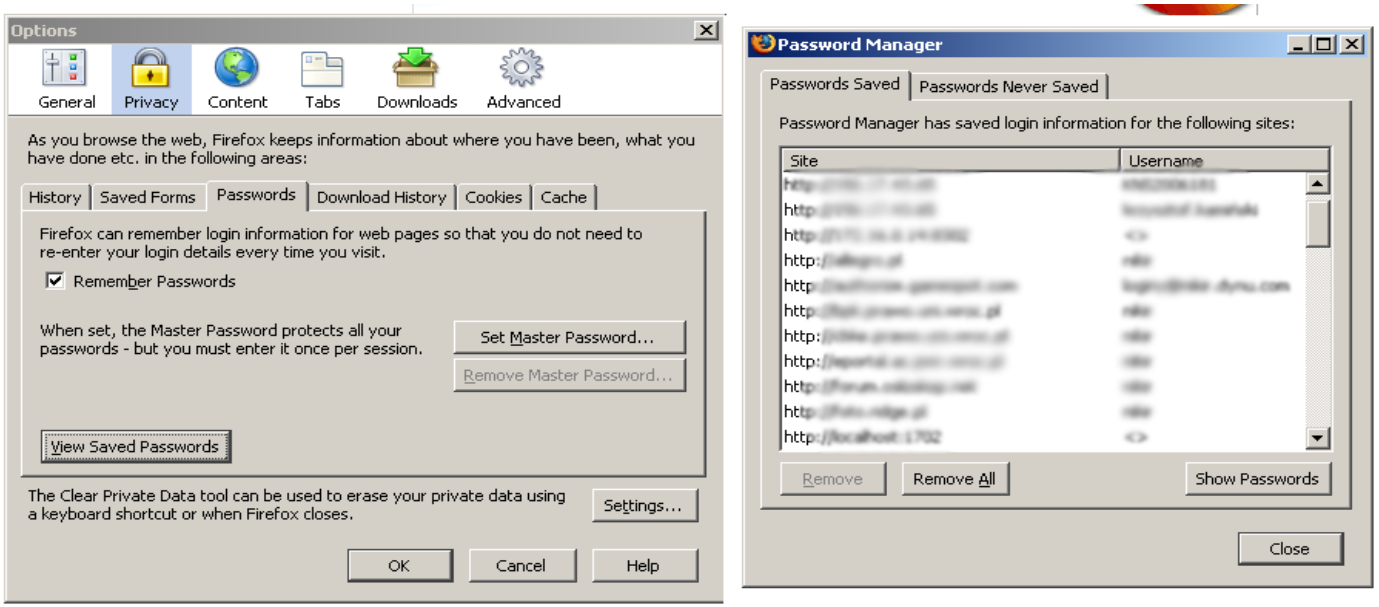


- Dlaczego logowanie przez SSL nie jest domyślne?

Sposoby bezpiecznego logowania na stronach WWW, c.d.

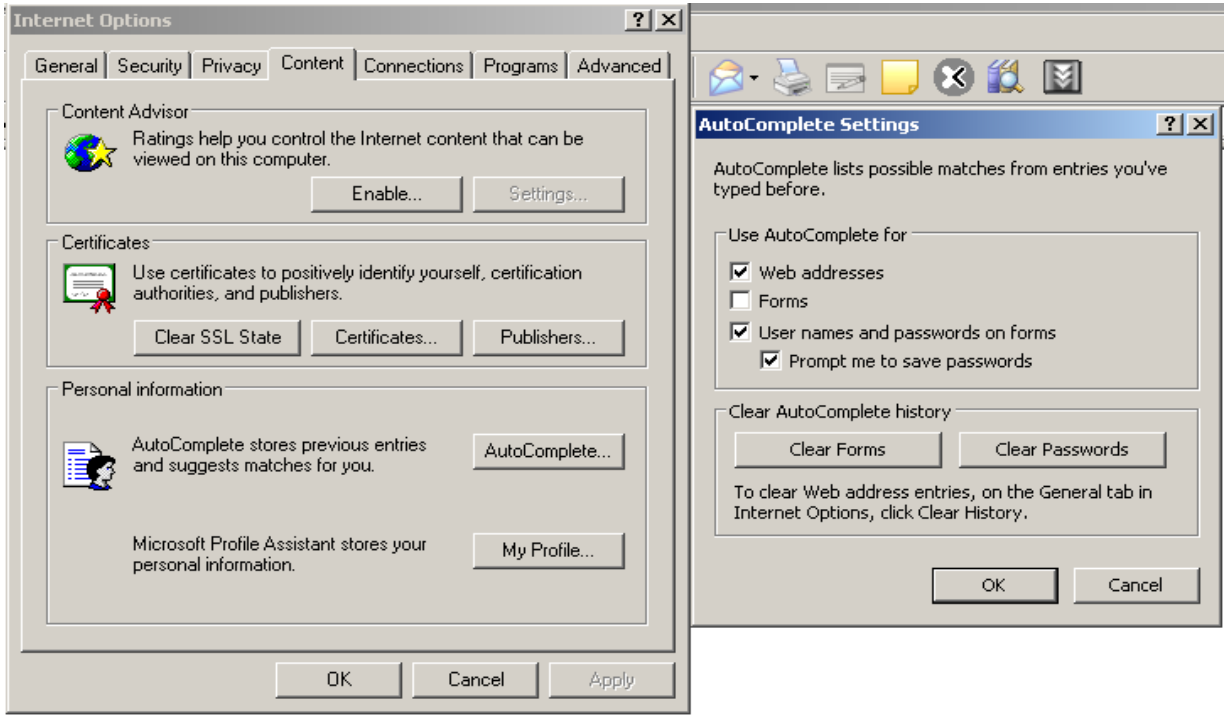
- Nigdy nie zapisywać w pamięci przeglądarki haseł do kont bankowych, poczty elektronicznej, itp.
- Komenda -> Usuń dane prywatne

Firefox



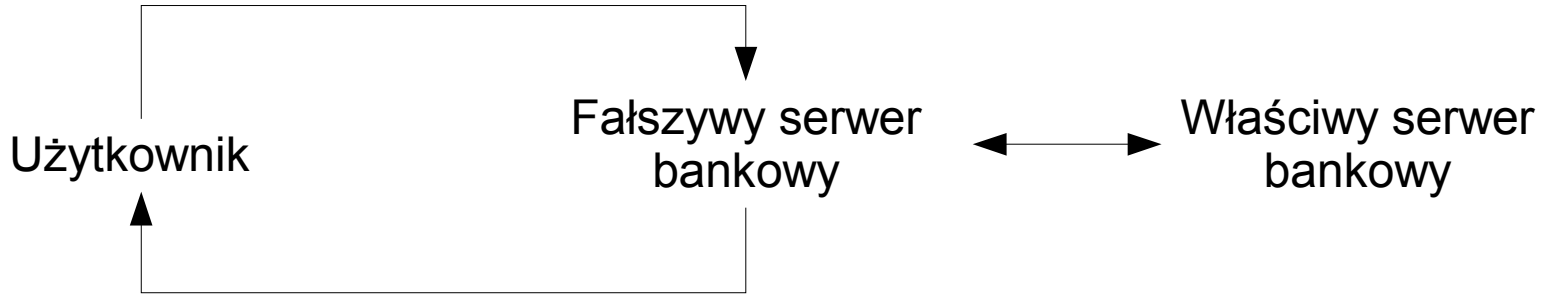
Sposoby bezpiecznego logowania na stronach WWW, c.d.

IE 6.0



Sposoby bezpiecznego logowania na stronach WWW, c.d.

- Szczególna ostrożność w przypadku kont bankowych
  - Hasła jednorazowe nie zabezpieczają w 100% przed kradzieżą pieniędzy



Bezpieczeństwo poczty elektronicznej

- Problemy
  - Kradzież kont
    - Używanie silnych haseł, nie logowanie się do skrzynek WWW z „niepewnych” stacji roboczych
    - Wpisywanie losowych znaków w pozycjach: przypomnienie hasła – pytanie/odpowiedź
    - Logowanie przez SSL

Bezpieczeństwo poczty elektronicznej

- Podsłuch
  - Tylko proces logowania do darmowych skrzynek typu: onet.pl, wp.pl jest zabezpieczony
  - Należy stosować kodowanie TLS/SSL w klientach pocztowych
- Podszywanie się
  - Zmora protokołu SMTP – nie ma możliwości identyfikacji nadawcy wiadomości email Rozwiązanie -> CERTYFIKATY CYFROWE

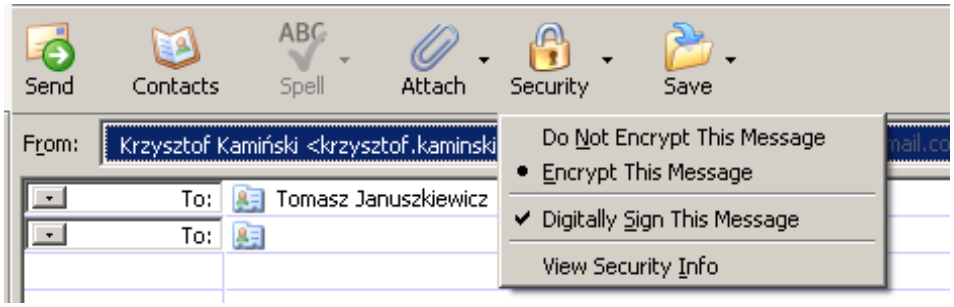
Bezpieczeństwo poczty elektronicznej

- Certyfikat darmowy – nie potwierdza pełnej tożsamości tylko dostęp do skrzynki email

www.thawte.com

Bezpieczeństwo poczty elektronicznej

- Możliwości certyfikatu
  - Podpis elektroniczny mail i załączników
  - Szyfrowanie całej wiadomości przy pomocy klucza publicznego adresata
    - W celu zaszyfrowania maila certyfikatem musi legitymować się adresat wiadomości



Komunikatory internetowe

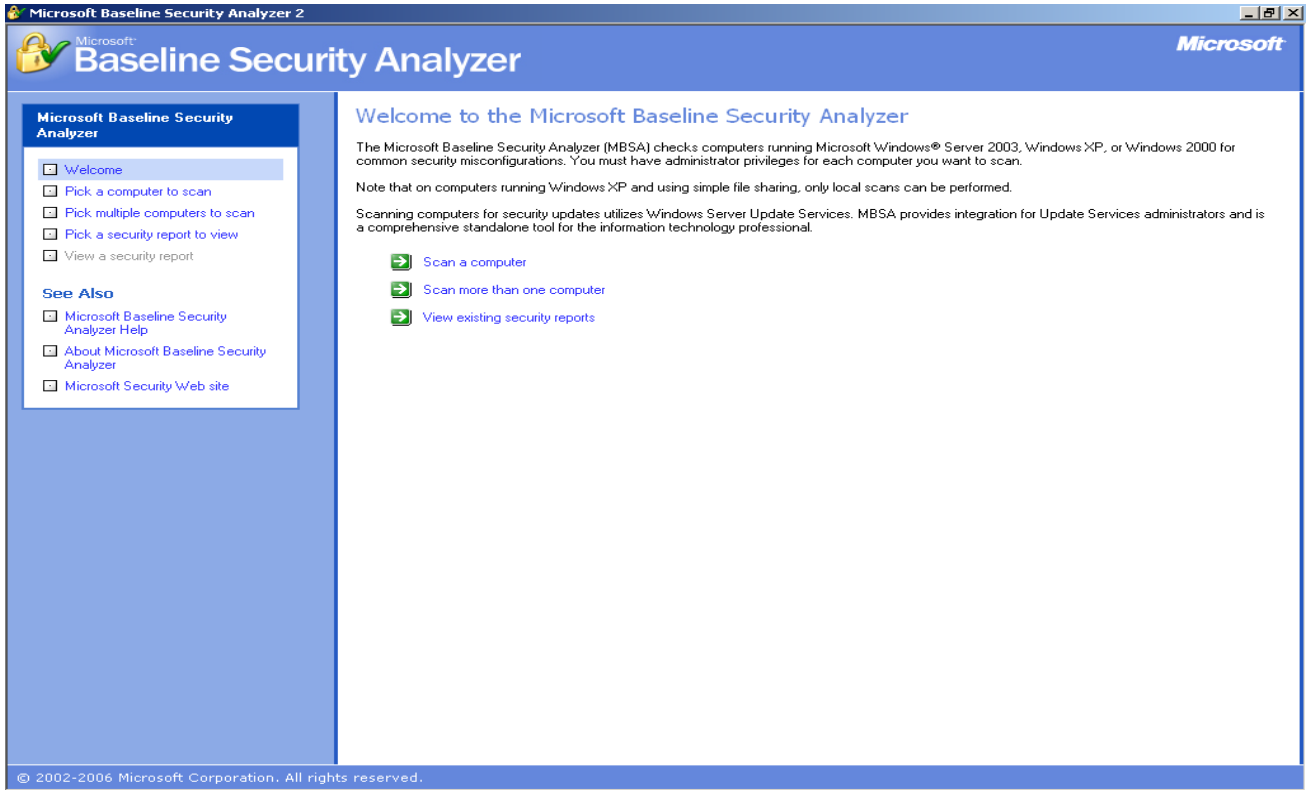
- GG, Tlen, WP Kontakt, itp. - transmisje szyfrują tylko niektóre wersje programów
- W celu sprawdzenia konkretnego programu warto użyć sniffer'a sieciowego i podsłuchać własny ruch
  - ethereal.com

Bezpieczeństwo systemu operacyjnego

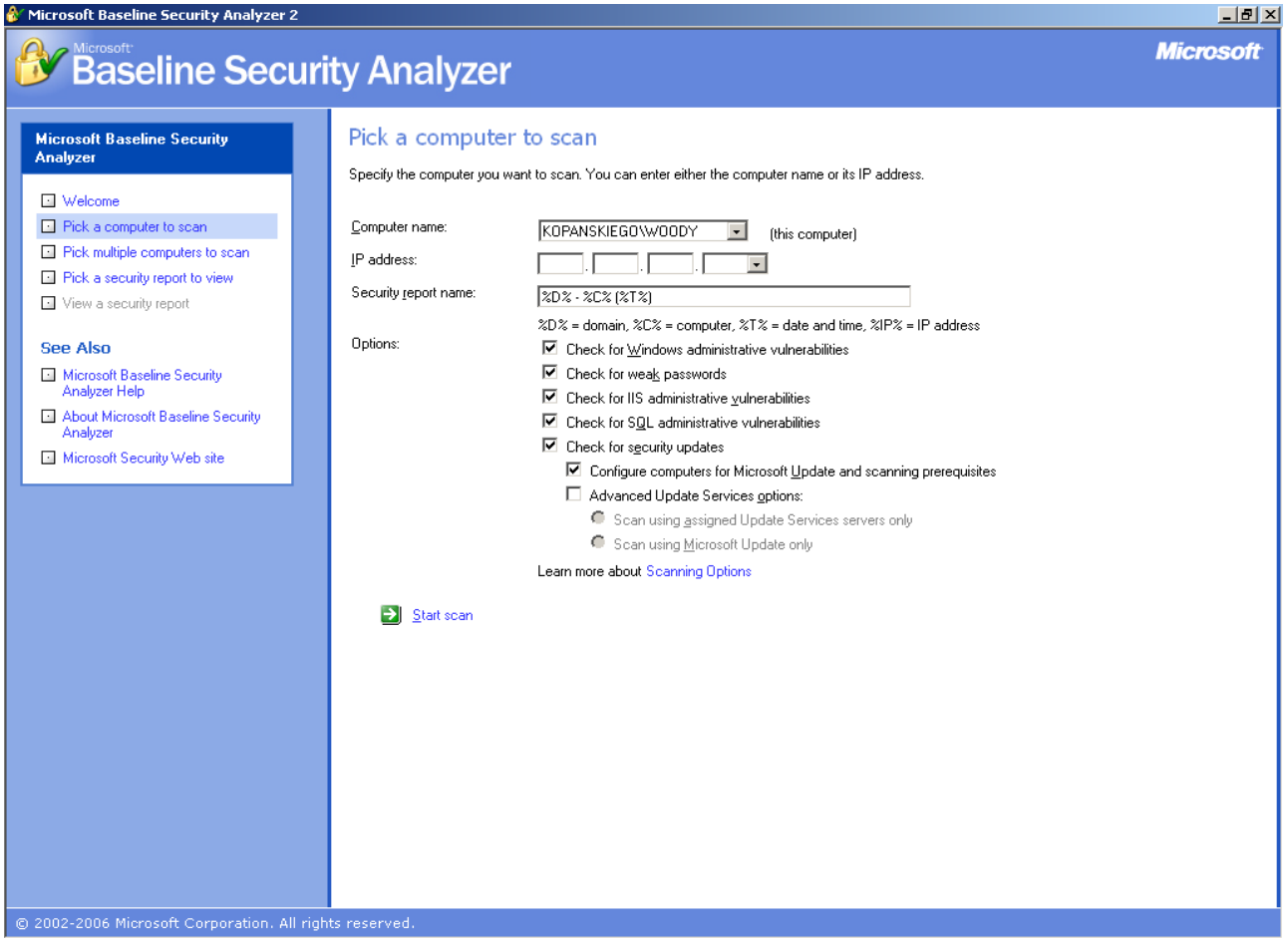
- Aktualizacje
- Włączony dostęp zdalny
- Włączone konto „GOŚĆ”
- Niezabezpieczone hasłem konto „ADMINISTRATOR”
- Brak oprogramowania antywirusowego
- Brak oprogramowania przeciw trojanom
- Brak silnych haseł na kontach

Microsoft Baseline Security Analyzer

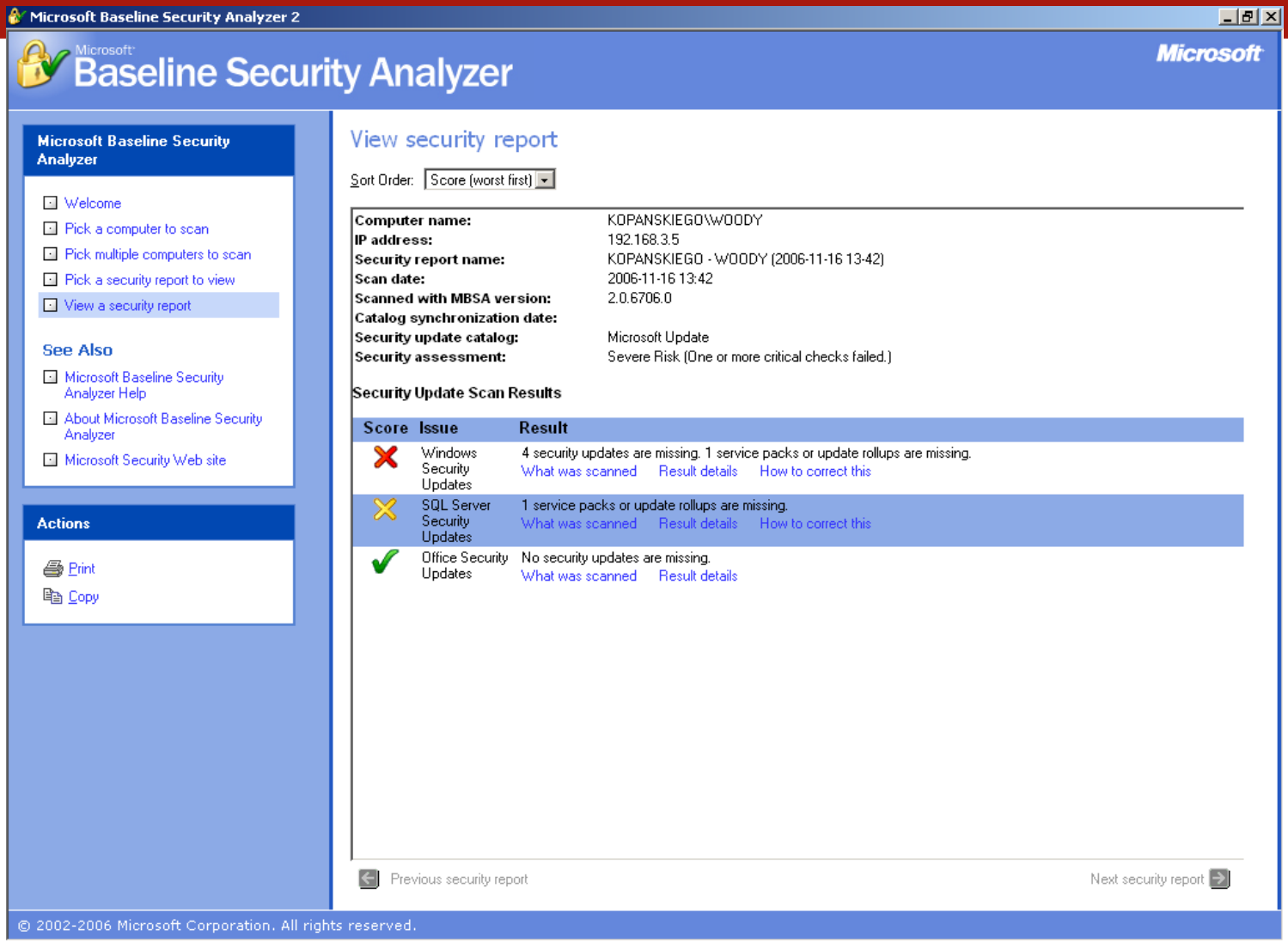
- Program umożliwiający kompleksowe badanie poziomu zabezpieczeń systemu i programów



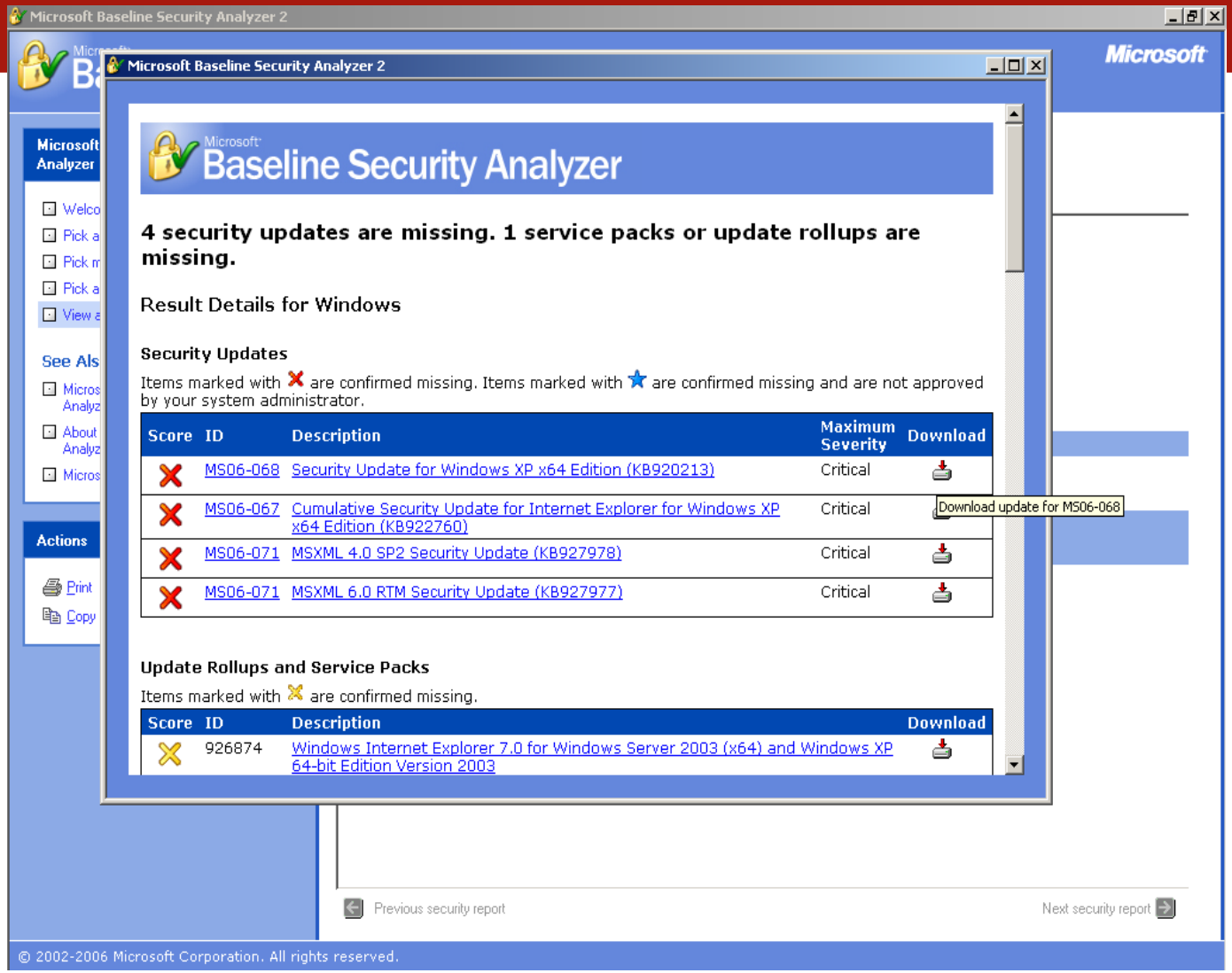
MBSA


Microsoft Baseline Security Analyzer 2
Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Pick a computer to scan
Specify the computer you want to scan. You can enter either the computer name or its IP address.
Computer name:
KOPANSKIEGO\WOODY
(this computer)
IP address:
Security report name:
%D% - %C% (%T%)
%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address
Options:
Check for Windows administrative vulnerabilities
Check for weak passwords
Check for IIS administrative vulnerabilities
Check for SQL administrative vulnerabilities
Check for security updates
Configure computers for Microsoft Update and scanning prerequisites
Advanced Update Services options:
Scan using assigned Update Services servers only
Scan using Microsoft Update only
Learn more about Scanning Options
Start scan
© 2002-2006 Microsoft Corporation. All rights reserved.

Krzysztof Kamiński – Komputer narzędziem w rękach prawnika



Krzysztof Kamiński – Komputer narzędziem w rękach prawnika



Zabezpieczenie danych na nośnikach typu PenDrive

- Scenariusz katastrofy
  - 1 prawnik
  - 1 klient
  - 1 zgubiony/ukradziony PenDrive z poufnymi danymi
- Rozwiązanie -> oprogramowanie szyfrujące dane na nośnikach przenośnych

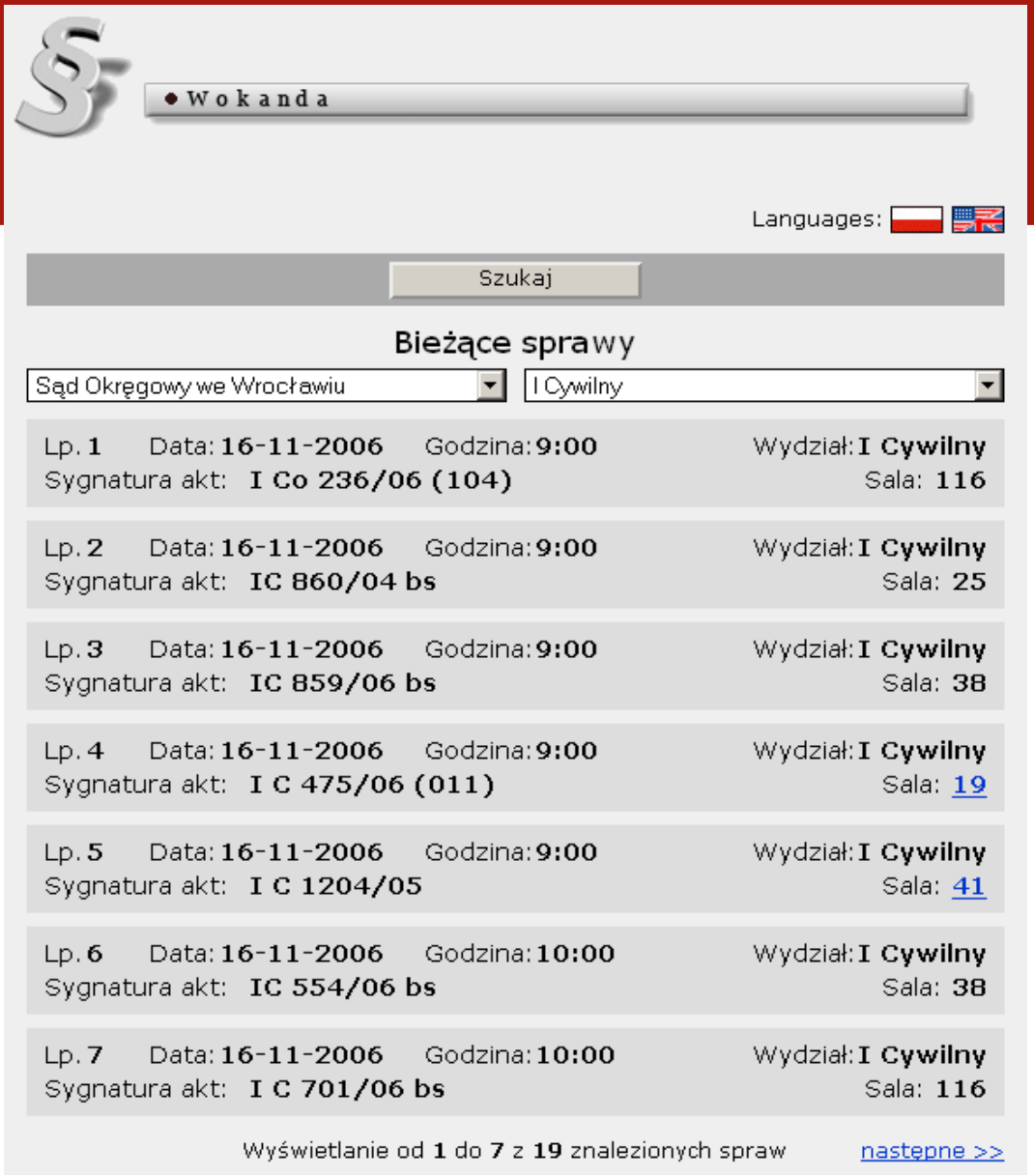
Zabezpieczenie danych na nośnikach typu PenDrive

- Oprogramowanie (darmowe) TrueCrypt
  - www.truecrypt.org
- Zalety:
  - Prostota obsługi (po lekkim treningu)
  - Bardzo wysoki poziom bezpieczeństwa
  - Wygoda
- Wady:
  - Konieczność pierwszego uruchomienia z uprawnieniami Administratora

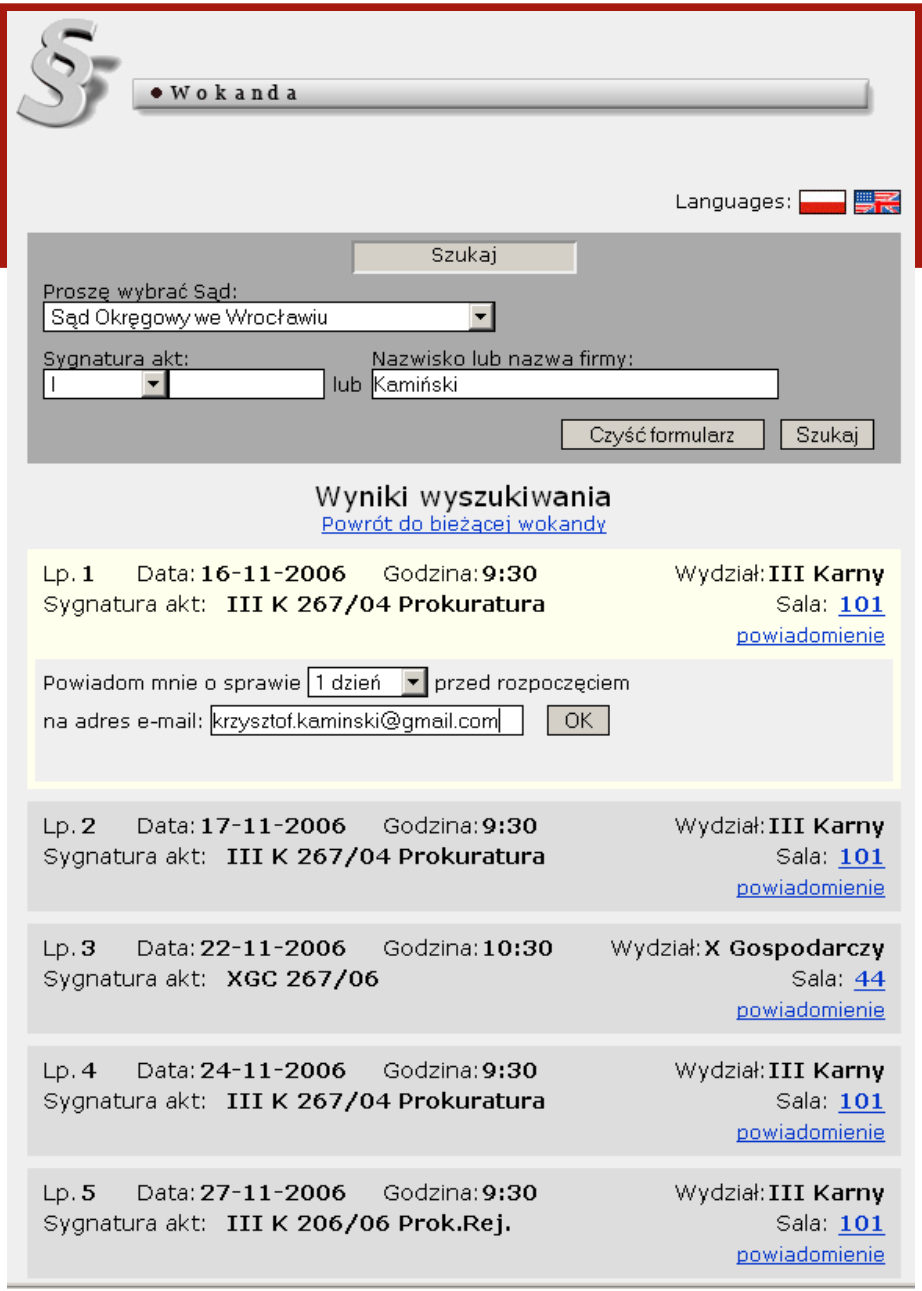
Systemy informatyczne w SO

- IUDEX – portal intranetowy SO
- Wokanda Elektroniczna – eWokanda
- Wokanda Internetowa – iWokanda
- System wspomagania pracy Sekretariatów – SINUS
- Dostęp do informacji prawniczej
  - LEX, LEXPOLONICA, LEGALIS

Krzysztof Kamiński – Komputer narzędziem w rękach prawnika



Krzysztof Kamiński – Komputer narzędziem w rękach prawnika



Dziękuję za uwagę!!
Pytania?