

PLATFORMA OBSŁUGI NAUKI **PLATON**



www.platon.pionier.net.pl



PLATON Ę U4 **Usługa powszechnej archiwizacji**

Łukasz Kuczyński
Dagmara Bubel
Lidia Szczygłowska



Projekt nr. POIG.02.03.00-00-028/08

DOTACJE NA INNOWACJE

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego



Celem usługi

PLATON U4 ó Usługi Powszechnej Archiwizacji

jest pomoc u ytkownikom i instytucjom w zabezpieczaniu ich danych

Usługa skierowana jest do:

- Uczelni, pracowników uczelni, naukowców
- Instytutów PAN i ich pracowników
- Centrów KDM, Operatorów Sieci MAN i krajowych (PIONIER)
- Szpitali klinicznych
- Wirtualnych laboratoriów i bibliotek cyfrowych

Docelowe zastosowanie:

” **Długoterminowa archiwizacja danych**

” **Kopie zapasowe**

” **Przechowywanie 2-go poziomu!!**

(ang. Secondary Storage)

(przy założeniu użytkowników mających lokalne systemy przechowywania)



Usługa **PLATON U4** oparta jest na oprogramowaniu **Krajowego Magazynu Danych**.

(KMD) oferuje dwie usługi wydajnego, wiarygodnego i bezpiecznego przechowywania danych:

- ” usług wirtualnego systemu plików
- ” aplikacji klienta kopii zapasowych i archiwizacji

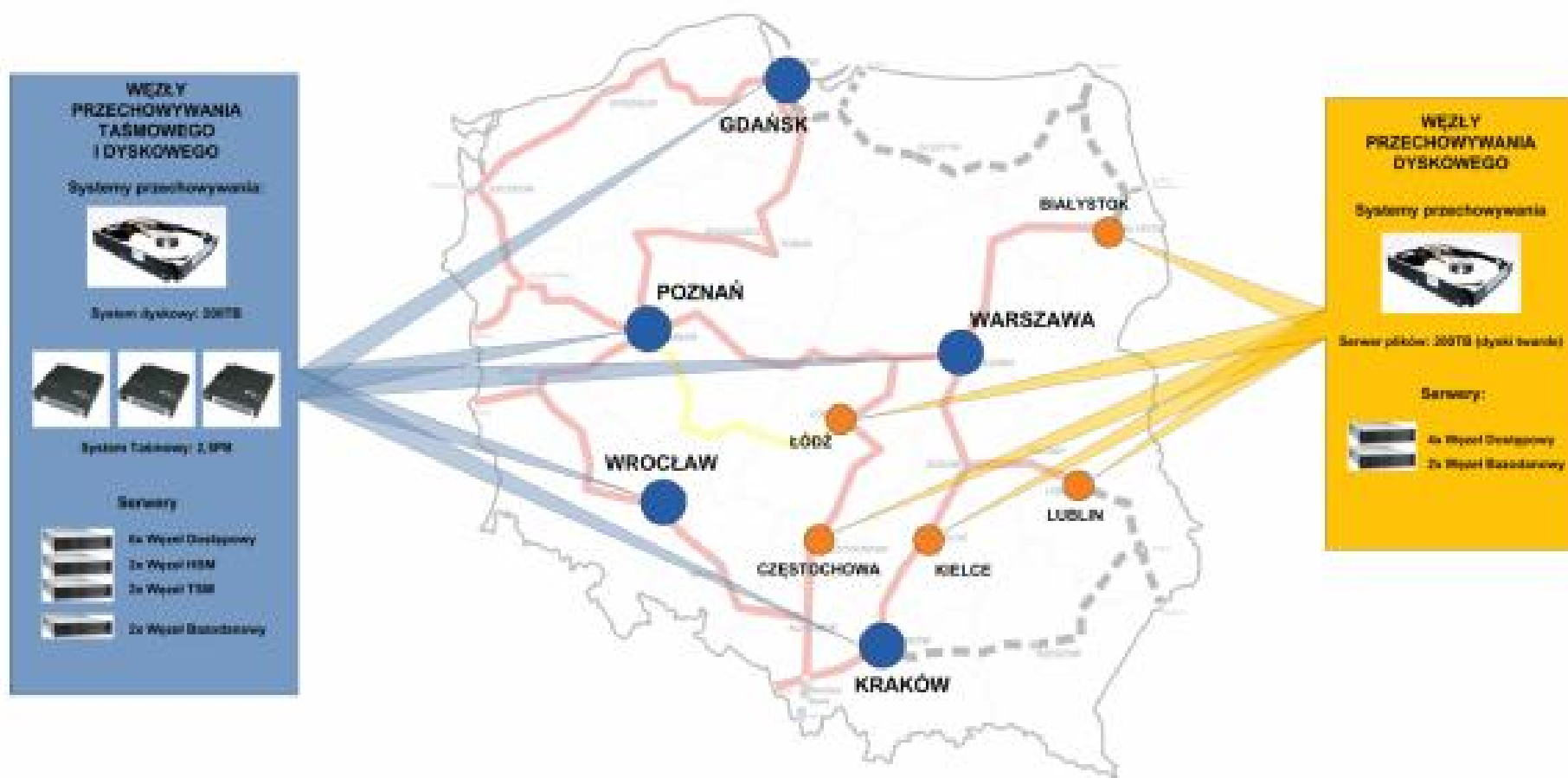


Podstawowe funkcje systemu

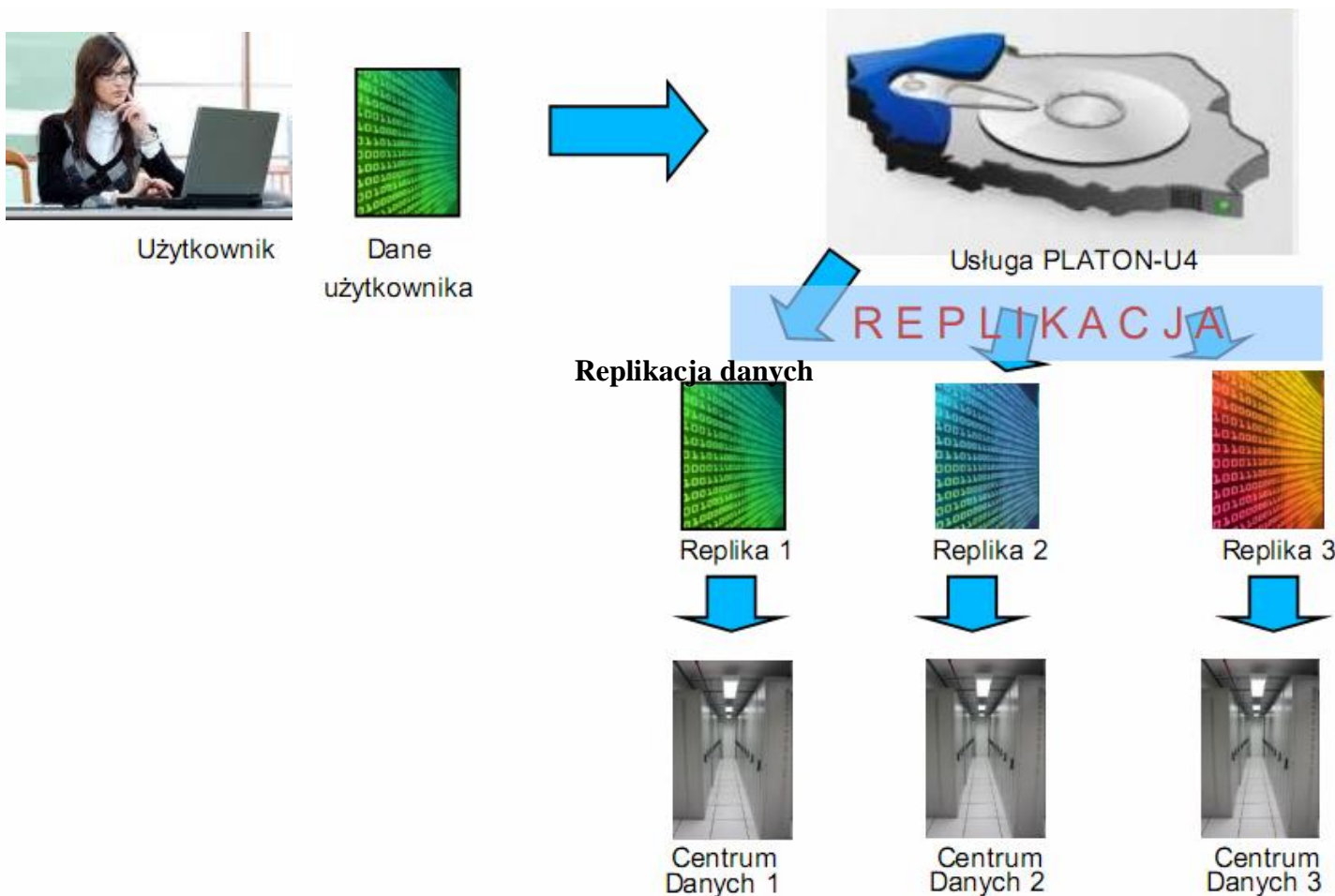
- ” Replikacja danych (min. 2 repliki)
- ” Wysoka trwałość danych
- ” Wysoka dostępność
- ” Rozproszenie systemu
- ” Skalowalność
- ” Unikanie centralnego punktu awarii
- ” Unikanie szkodliwych ataków
- ” Wiele punktów dostępu do danych



Schemat infrastruktury Usługi Powszechnej Archiwizacji



Wysoka dostępność dzięki replikacji



Replikacja danych

Replikacja synchroniczna

ÉDłszy czas odpowiedzi systemu

ÉPewno dot. stanu/ spójno ci wszystkich replik



Replikacja asynchroniczna

ÉKrótszy czas odpowiedzi systemu

ÉPewno dot. stanu / spójno ci tylko dla 1. repliki



=?



W architekturze KMD/PLATON-U4 obsługiwane s obydwa tryby replikacji!

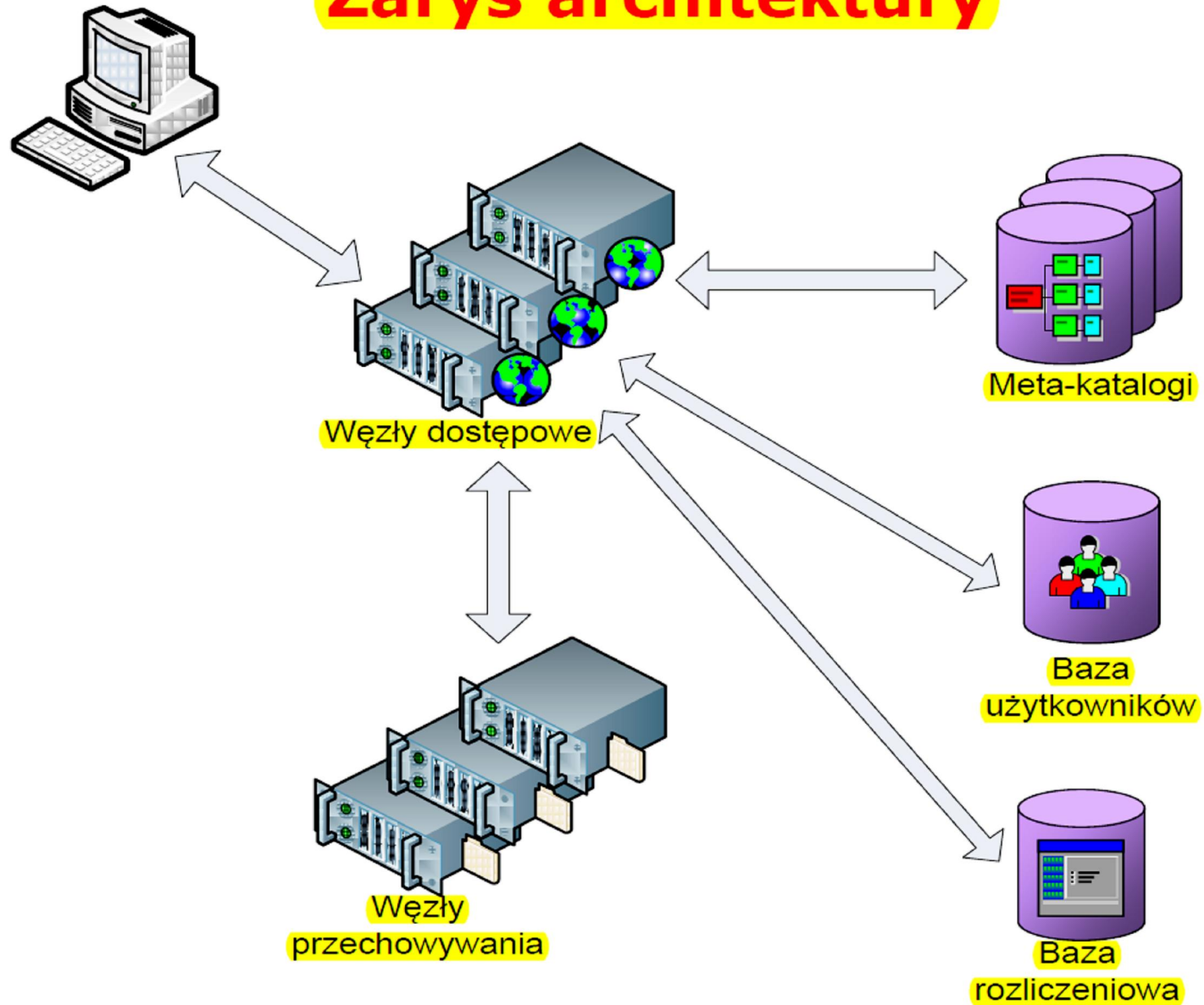
PLATON-U4: bezpieczeństwo danych

- **Bezpieczeństwo danych:**

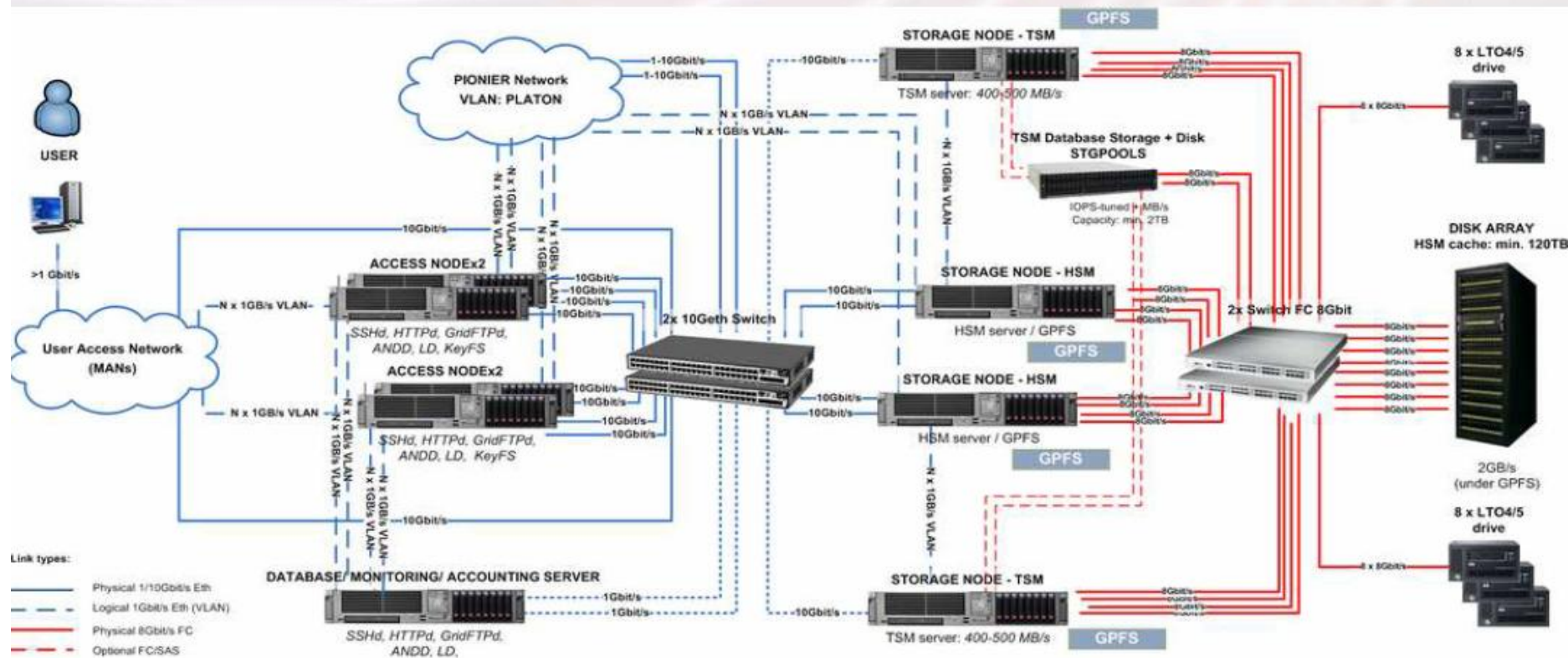
- Dane szyfrowane w drodze do systemu:
 - » SSH,
 - » HTTPS...
- Dane szyfrowane wewnątrz systemu:
 - » Łąca zabezpieczone kryptograficznie
- Dane przechowywane na szyfrowanych mediach:
 - » Sprzętowe szyfrowanie w technologii taśmowej LTO4
- Fizyczne bezpieczeństwo danych:
 - » Centra Danych z kontrolą dostępu
 - » Trwałość danych/mediów gwarantowana przez warunki środowiskowe



Zarys architektury



PLATON-U4: Realizacja usługi taśmowe węzły składowania



Dostęp do danych

Standardowe protokoły dostępu do danych i meta-danych

” Po stronie użytkownika o typowe oprogramowanie klienckie:

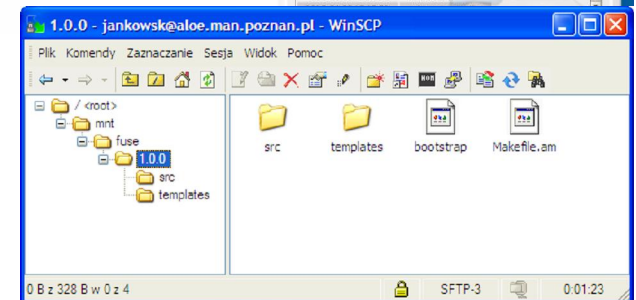
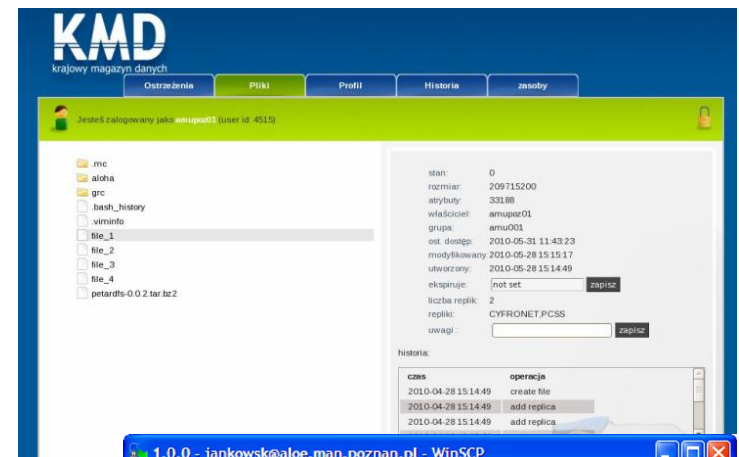
• SSH/SFTP (WinSCP, SSHFS)

• HTTP/WebDAV (przeładowarka internetowa, klient WebDav,

mapowanie dysków w Windows)

• GridFTP

” Po stronie systemu obsługiwane systemy plików z danymi i meta-danymi



Index of /dav

[ICO]	Name	Last modified	Size	Description
[DIR]	Parent Directory			-
[DIR]	aloha/	31-May-2010 15:36		-
[]	file_1	28-May-2010 15:15	200M	
[]	file_2	28-May-2010 15:16	200M	
[]	file_3	28-May-2010 15:17	200M	
[]	file_4	28-May-2010 15:17	200M	
[DIR]	grc/	01-Jun-2010 12:29		-
[]	petardfs-0.0.2.tar.bz2	31-May-2010 11:45	284K	

Narzędzia klienta

” Dostęp przez stronę www:

- . Interfejs www użytkownika
- . Certyfikaty użytkownika i połączenie szyfrowane



” Dostęp przez dysk sieciowy WebDAV:

- . Bezpośredni dostęp do danych
- . Możliwość podłączenia jako dysk

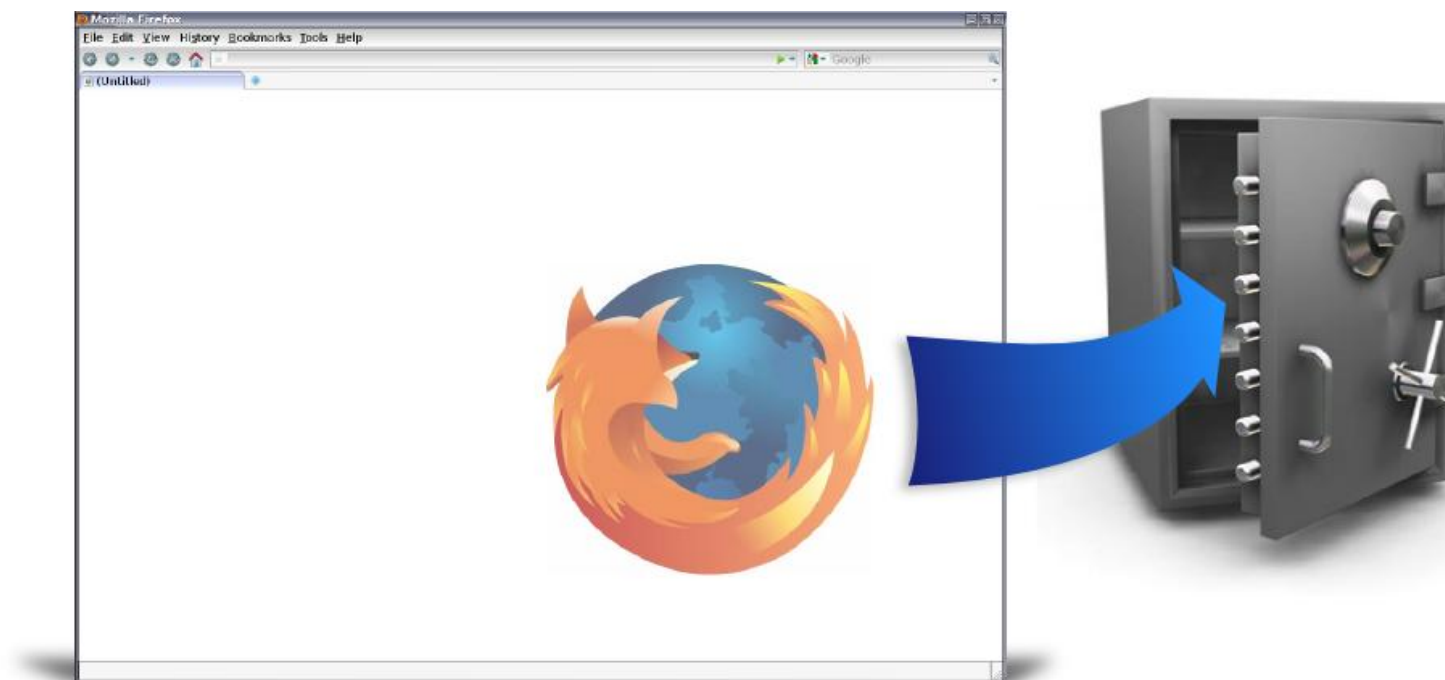


” Dostęp przez protokół SSH:

- . Wykorzystanie narzędzia WinSCP
- . Wykorzystanie narzędzia SSHFS i SFTP

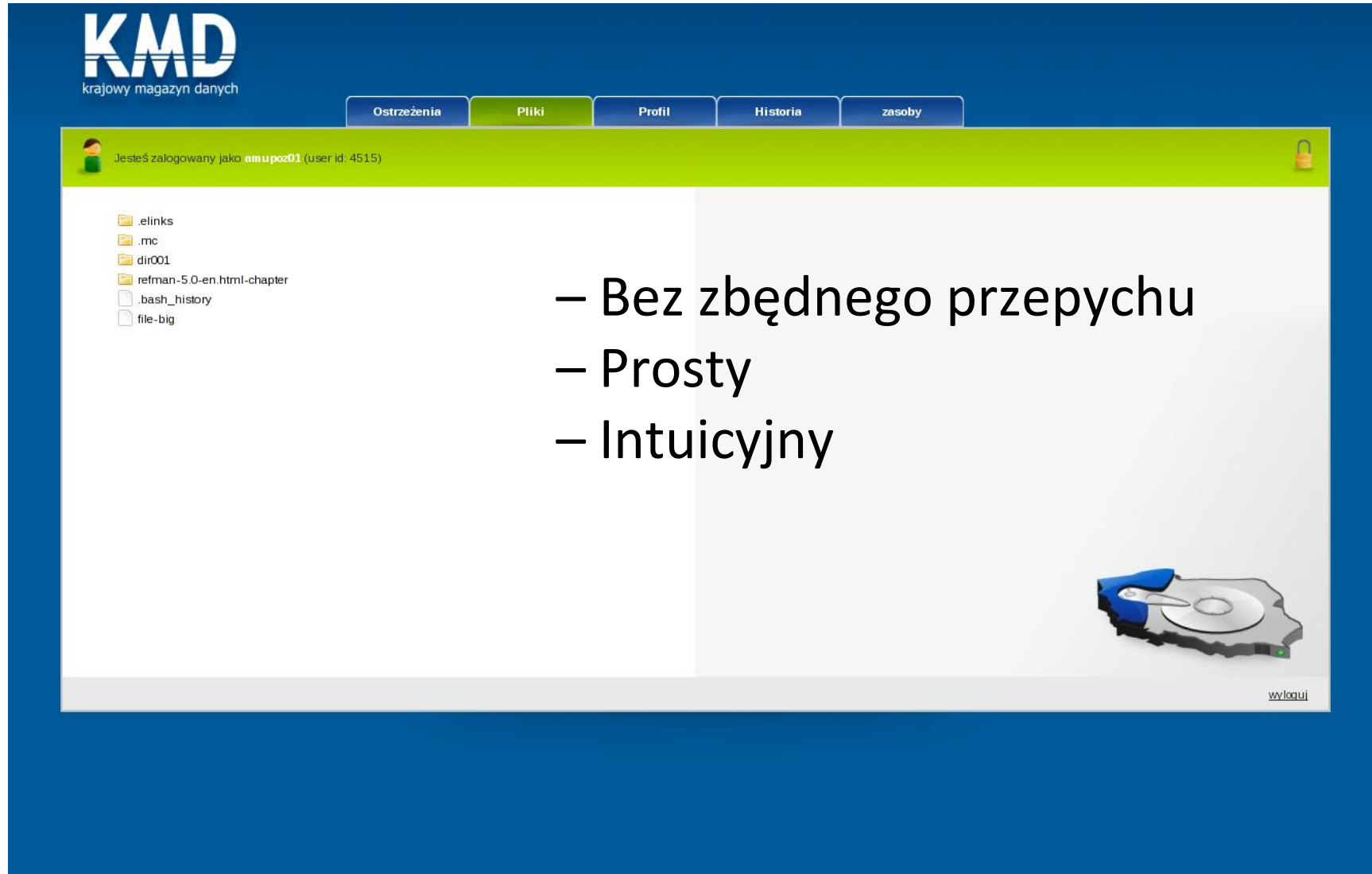


Dostęp do danych przez interfejs www



Standardowa przeglądarka Firefox

Interfejs www



KMD
krajowy magazyn danych

Ostrzeżenia Pliki Profil Historia zasoby

Jesteś zalogowany jako **amupoz01** (user id: 4515)

- .elinks
- .mc
- dir001
- refman-5.0-en.html-chapter
- .bash_history
- file-big

– Bez zbędnego przepychu
– Prosty
– Intuicyjny

[wylouj](#)

Interfejs www – pogląd plików

The screenshot shows the KMD (Krajowy Magazyn Danych) web interface. At the top, there is a navigation menu with buttons for 'Ostrzeżenia', 'Pliki', 'Profil', 'Historia', and 'zasoby'. The user is logged in as 'amu001' (user id: 4515). The main content area is divided into two sections:

- Pliki:** A file directory view showing the path 'home > dir001'. The files listed are: 'dir', 'refman-5.0-en.html-chapter', '2', 'accounting.txt', 'file-big', and 'nds.log.1'. This section is circled in red.
- Metadane:** A detailed view of the selected file's metadata. This section is also circled in red. It includes fields for: stan (0), rozmiar (131981), atrybuty (33206), właściciel (amu001), grupa (amu001), ośt. dostęp (2010-05-10 11:01:09), modyfikowany (2010-05-14 17:25:00), utworzony (2010-05-18 14:47:05), expiruje (not set), liczba replik (2), repliki (CYFRONET,PCSS), and uwagi. There are 'zapisz' buttons for the 'ekspiruje' and 'uwagi' fields. Below the metadata is a 'historia' table showing a list of operations.

czas	operacja
2010-04-18 14:47:04	create file
2010-04-18 14:47:04	add replica
2010-04-18 14:47:04	add replica
2010-04-18 14:47:05	unknown operation

At the bottom right of the metadata section, there is a 'pobierz' button with a download icon and a 'wzrost' button with an upward arrow icon. The interface also features a 'wwloguj' link at the bottom right.

Interfejs www – metadane...

The screenshot shows the KMD (Krajowy Magazyn Danych) web interface. The user is logged in as amupoz01. The interface displays a file browser on the left and a metadata editor on the right. The metadata editor shows various fields such as stan, rozmiar, atrybuty, właściciel, grupa, and dates. A red circle highlights the 'liczba replik' field, which is set to 2. Below this, there is a field for 'repliki' containing 'CYFRONET,PCSS'. A 'historia' table shows a list of operations performed on the file.

Dokąd trafiają repliki

czas	operacja
2010-04-18 14:47:04	create file
2010-04-18 14:47:04	add replica
2010-04-18 14:47:04	add replica
2010-04-18 14:47:05	unknown operation

Interfejs www – metadane...

KMD
krajowy magazyn danych

Ostrzeżenia | **Pliki** | Profil | Historia | zasoby

Jesteś zalogowany jako **amupoz01** (user id: 4515)

ścieżka: home ▶ dir001

- ↑ ..
- dir
- refman-5.0-en.html-chapter
- 2
- accounting.txt
- file-big
- nds.log.1

stan: 0
rozmiar: 131981
atrybuty: 33206
właściciel: amupoz01
grupa: amu001
ost. dostęp: 2010-05-10 11:01:09
modyfikowany: 2010-05-14 17:25:00
utworzony: 2010-05-18 14:47:05
ekspiruje:
liczba replik: 2
repliki: C:\PROM\...
uwagi :

historia:

czas	operacja
2010-04-18 14:47:04	create file
2010-04-18 14:47:04	add replica
2010-04-18 14:47:04	add replica
2010-04-18 14:47:05	unknown operation

www.loqui

Uwagi – dodatkowy opis pliku

Interfejs www – wykorzystanie zasobów

KMD
krajowy magazyn danych

Ostrzeżenia

Pliki

Profil

Historia

zasoby



Jesteś zalogowany jako **amupoz01** (user id: 4515)



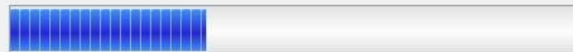
Domyślne repliki:

organizacja: PCSS
organizacja: WCSS
organizacja: Cyfronet

Dodatkowe repliki:

organizacja: TASK

Zajęta przestrzeń: 34% (0 B z 155 GB)



Wykorzystanie limitu plików: 66% (z 232783872)



Wykorzystanie limitu katalogów: 14% (z 57671680)



Interfejs www – profil użytkownika

KMD
krajowy magazyn danych

Ostrzeżenia

Pliki

Profil

Historia

zasoby



Jesteś zalogowany jako **amupoz01** (user id: 4515)



nazwa instytucji:	Uniwersytet im. Adama Mickiewicza w Poznaniu
opis:	Kontrakt AMU-001
nazwa organizacji:	PCSS
NIP:	777-000-63-50
adres:	ul.Wieniawskiego 1, 61-712, Poznań
adres do korespondencji:	..
adres e-mail:	office@amu.edu.pl
opis kontraktu:	Kontrakt AMU-001
ostatnia aktywnosc:	
liczba wymaganych replik:	2
sposob realizacji replikacji:	synchroniczna
maksymalny transfer:	132070244352
miękką quota:	123 GB
twarda quota:	155 GB
limit plików:	232783872
limit katalogów:	57671680
adres zasobów webdav:	https://10.0.6.212:14515/dav/



[wyloguj](#)

Interfejs www – profil użytkownika

Jesteś zalogowany jako **amupoz01** (user id: 4515)

nazwa instytucji:	Uniwersytet im. Adama Mickiewicza w Poznaniu
opis:	Kontrakt AMU-001
nazwa organizacji:	PCSS
NIP:	777-000-63-50
adres:	ul. Wieniawskiego 1, 61-712, Poznań
adres do korespondencji:	..
adres e-mail:	office@amu.edu.pl
opis kontraktu:	Kontrakt AMU-001
ostatnia aktywnosc:	
liczba wymaganych replik:	2
sposób realizacji replikacji:	synchroniczna
maksymalny transfer:	132070244352
mięka quota:	123 GB
twarda quota:	155 GB
limit plików:	232783872
limit katalogów:	57671680
adres zasobów webdav:	https://10.0.6.212:14515/dav/

Kim jestem

Ile razy replikowane są moje dane

Adres do zasobów WebDAV

Bezpieczeństwo

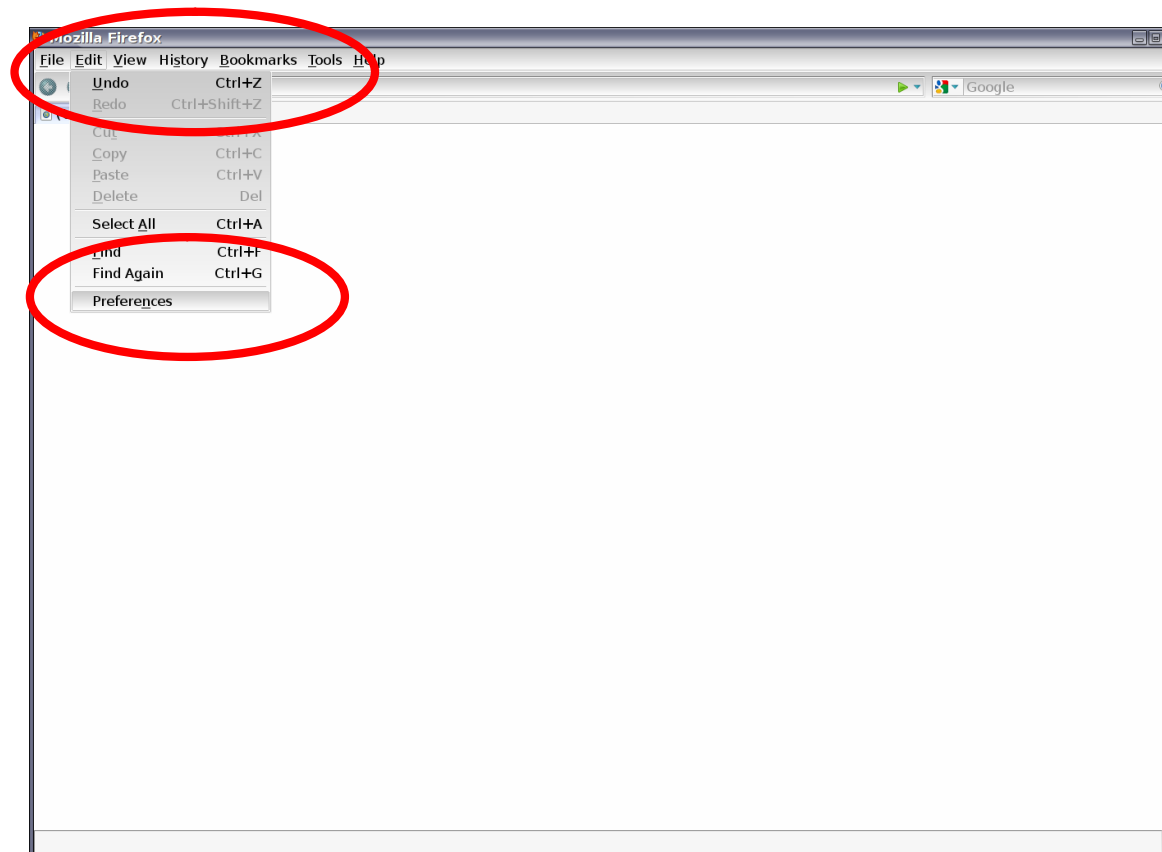
- “ Wszystkie połączenia z KMD są szyfrowane
- “ Autoryzacja użytkownika następuje na podstawie jego certyfikatu wystawionego przez CA
- “ Nie trzeba pamiętać „loginu” i hasła
- “ Nie trzeba przyklejać informacji o dostępie do konta na monitorze
- “ Możliwość wprowadzenia kart lub kluczy USB z certyfikatem

Instalacja certyfikatu użytkownika w przeglądarce (1)

- Edycja
- Preferencje

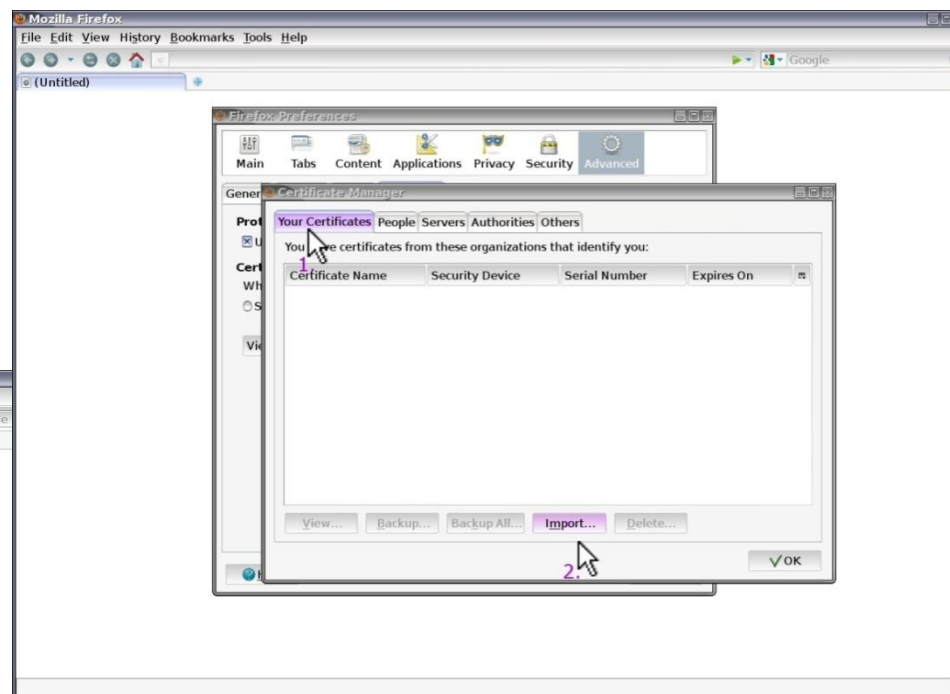
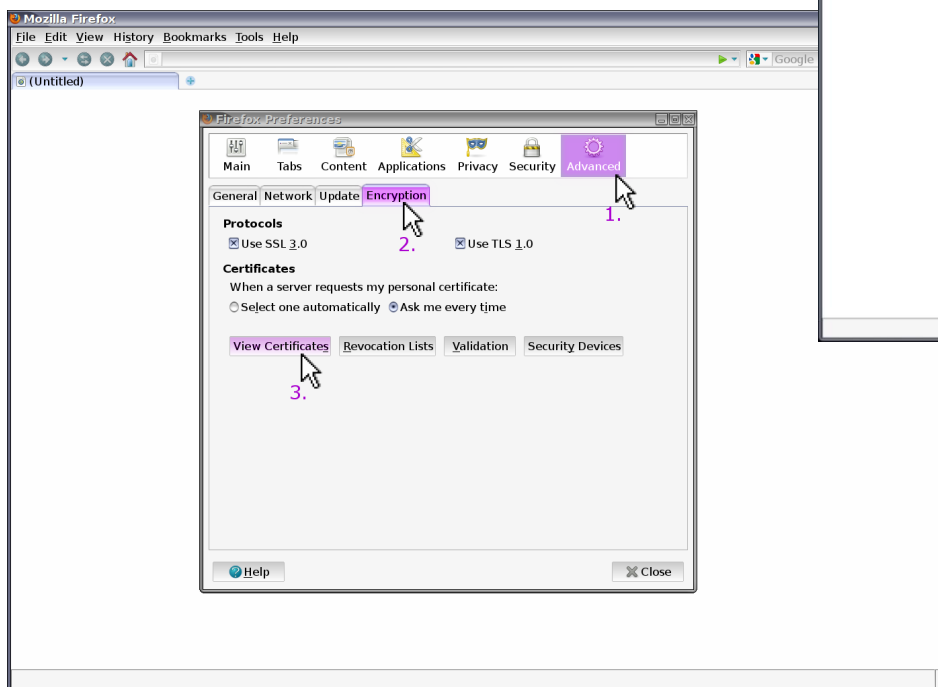
lub

- Narzędzia
- Opcje



Instalacja certyfikatu w przeglądarce (2, 3)

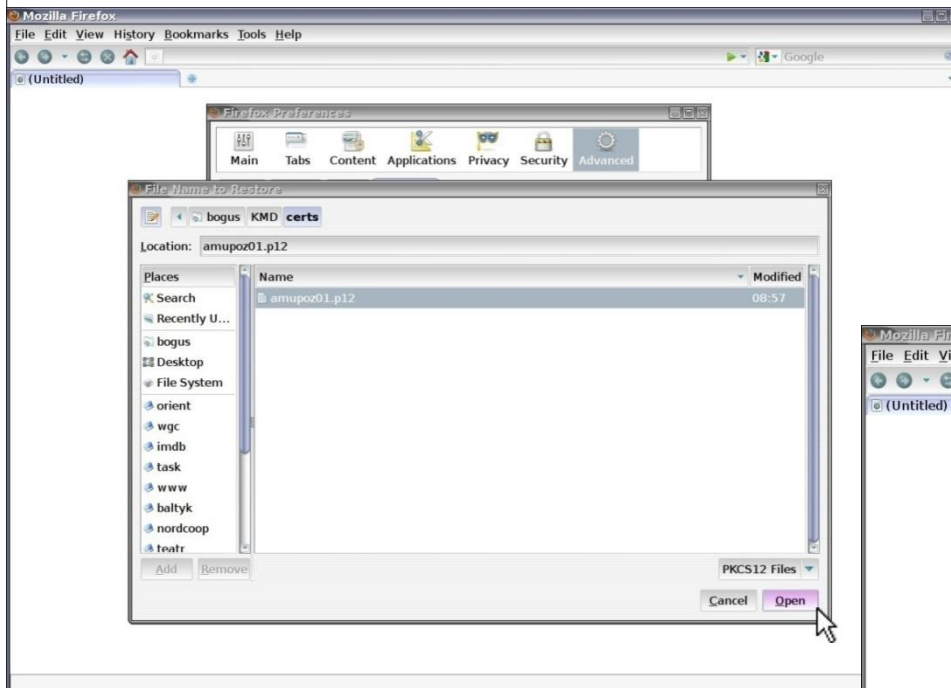
1. Zaawansowane
2. Szyfrowanie
3. Wyświetlenie certyfikatów



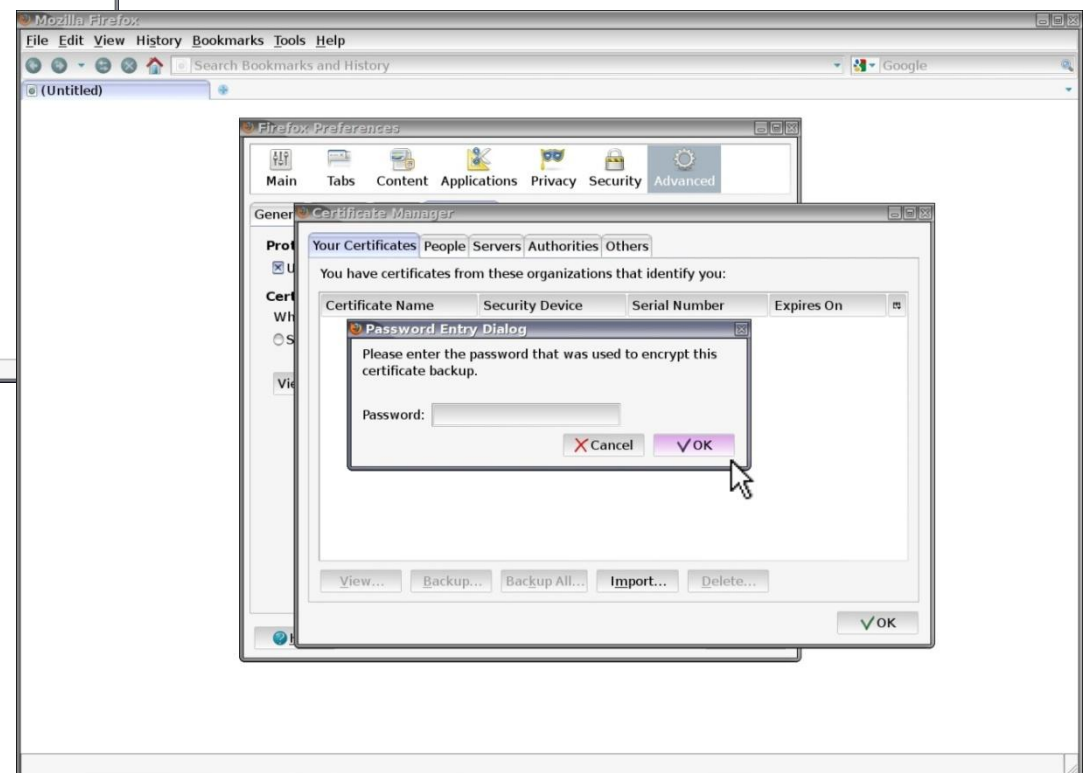
1. Twoje certyfikaty
2. Importuj

Instalacja certyfikatu w przeglądarce (4, 5)

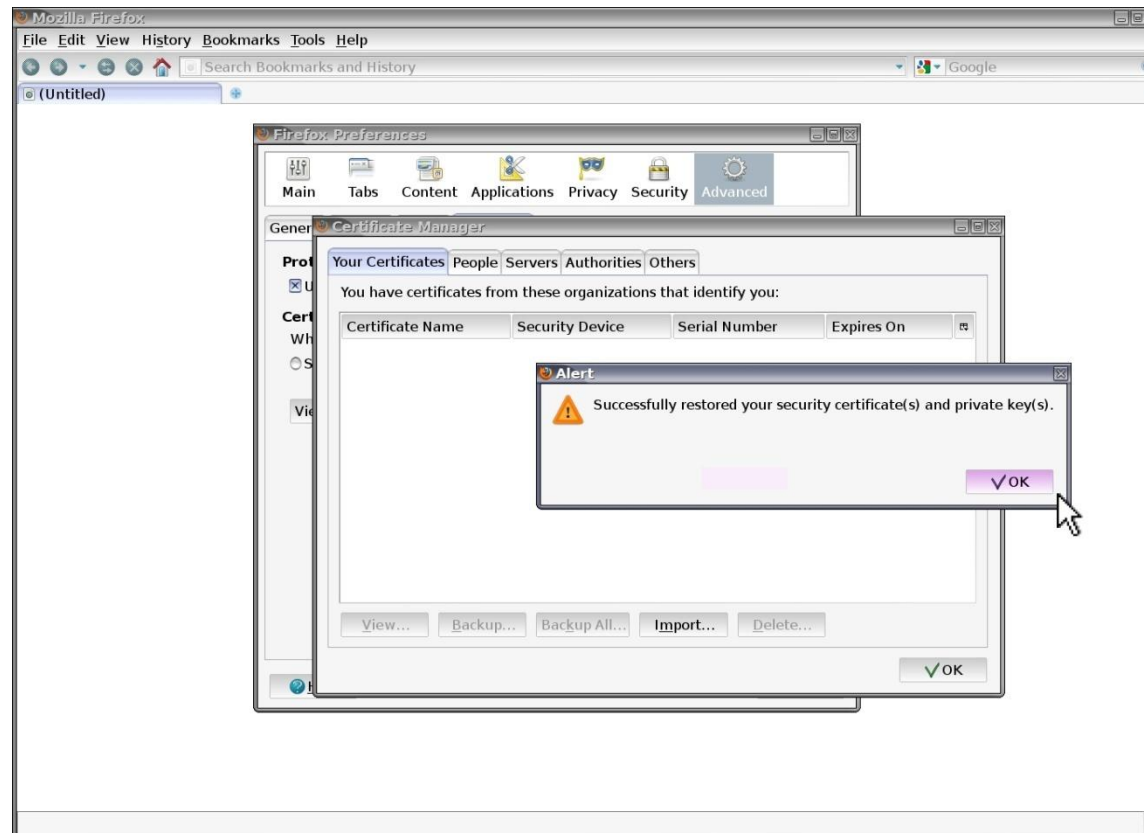
Jeśli certyfikat zabezpieczony jest hasłem, to należy je podać



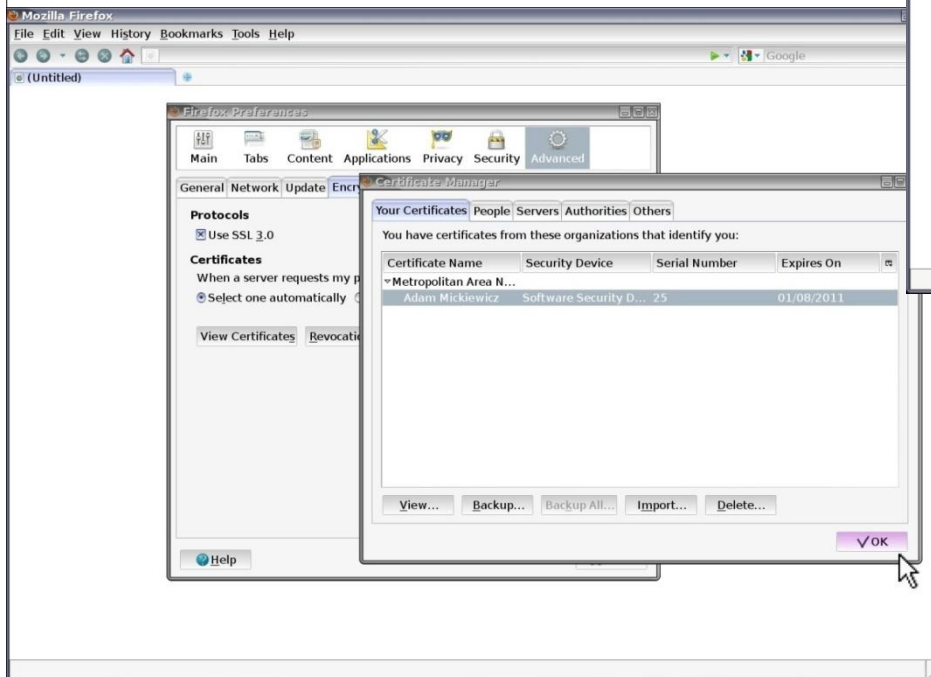
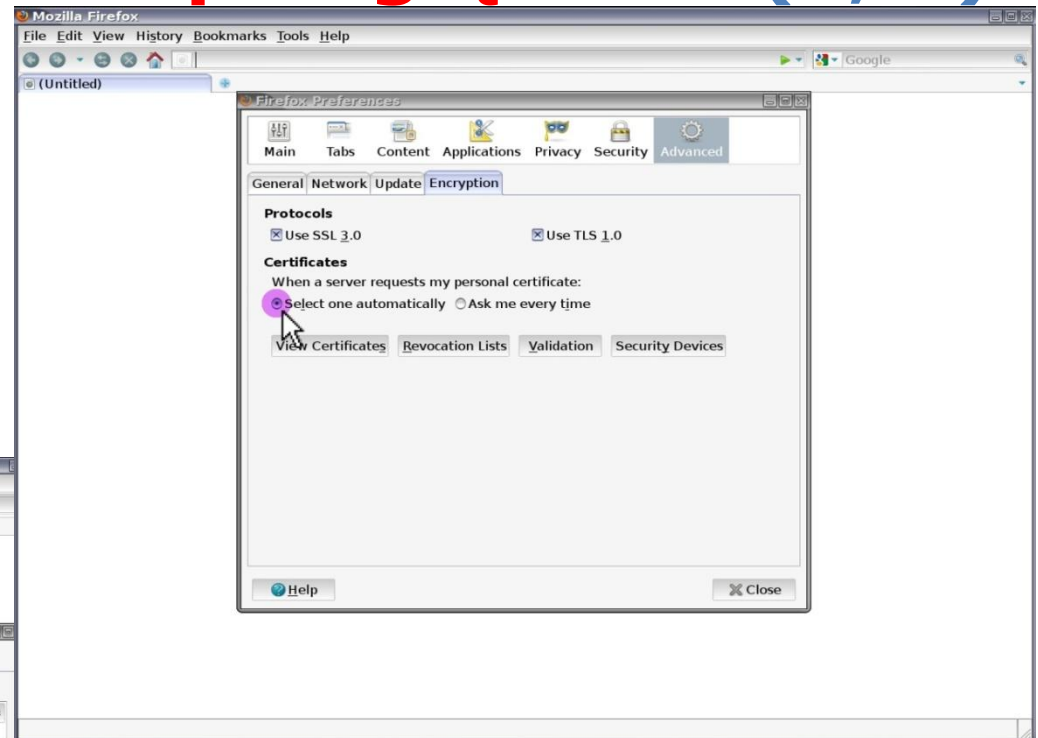
1. Wybieramy plik z certyfikatem
2. Otwórz



Instalacja certyfikatu w przeglądarce (6)



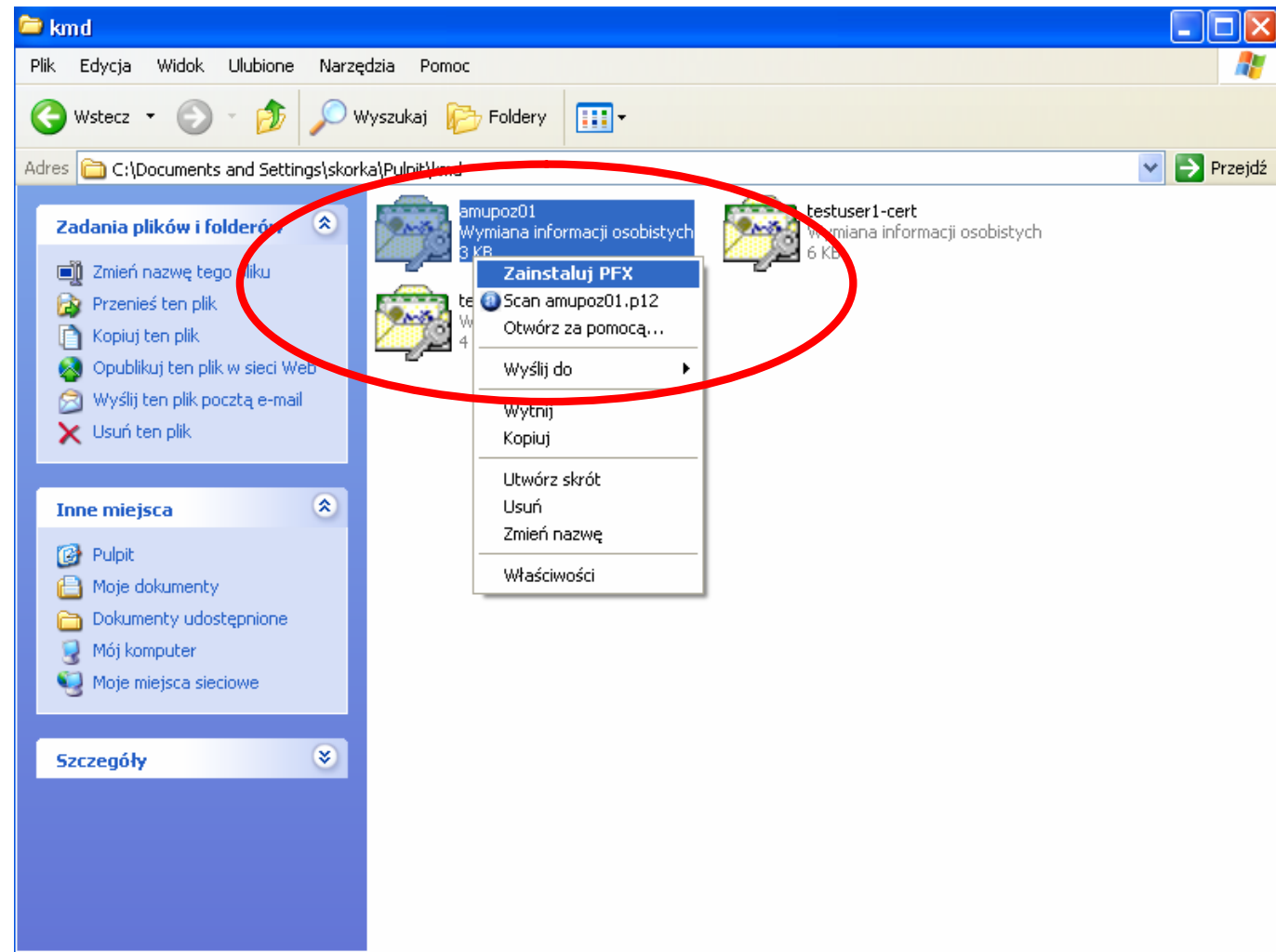
Instalacja certyfikatu w przeglądarce (7, 8)



Aby ułatwić dostęp p
zaznacz Wybierz
certyfikat
automatycznie

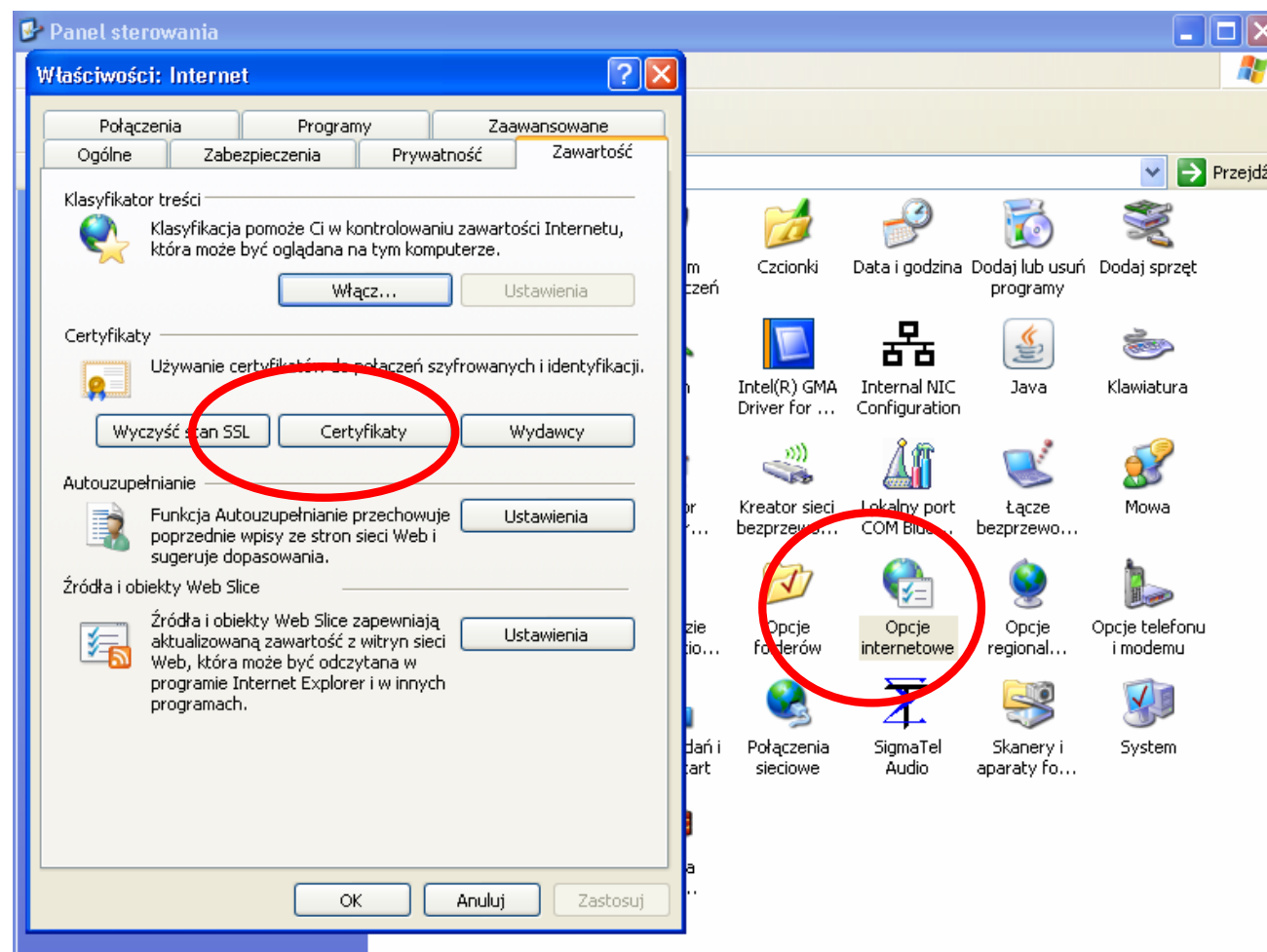
Instalacja certyfikatu w systemie Windows

Wystarczy
kliknąć
prawym
klawiszem
myszy



Edycja certyfikatów w systemie Windows

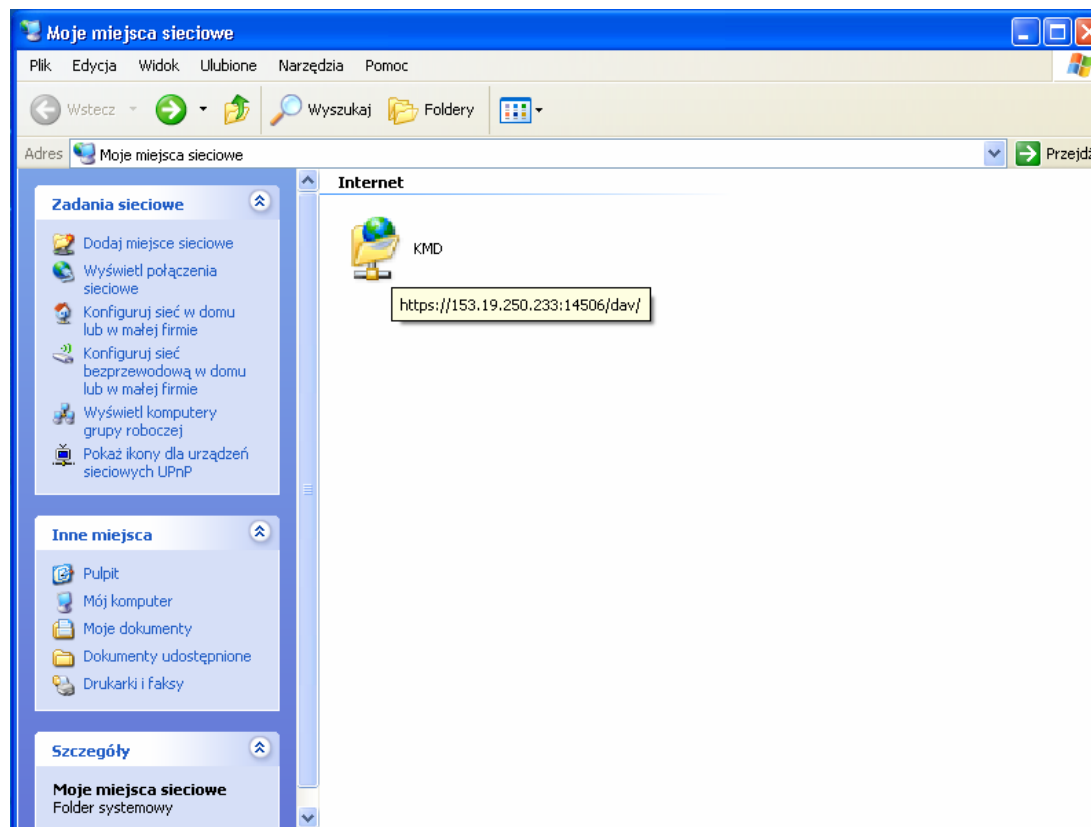
1. Panel sterowania
2. Opcje Internetowe
3. Zawartość
4. Certyfikaty



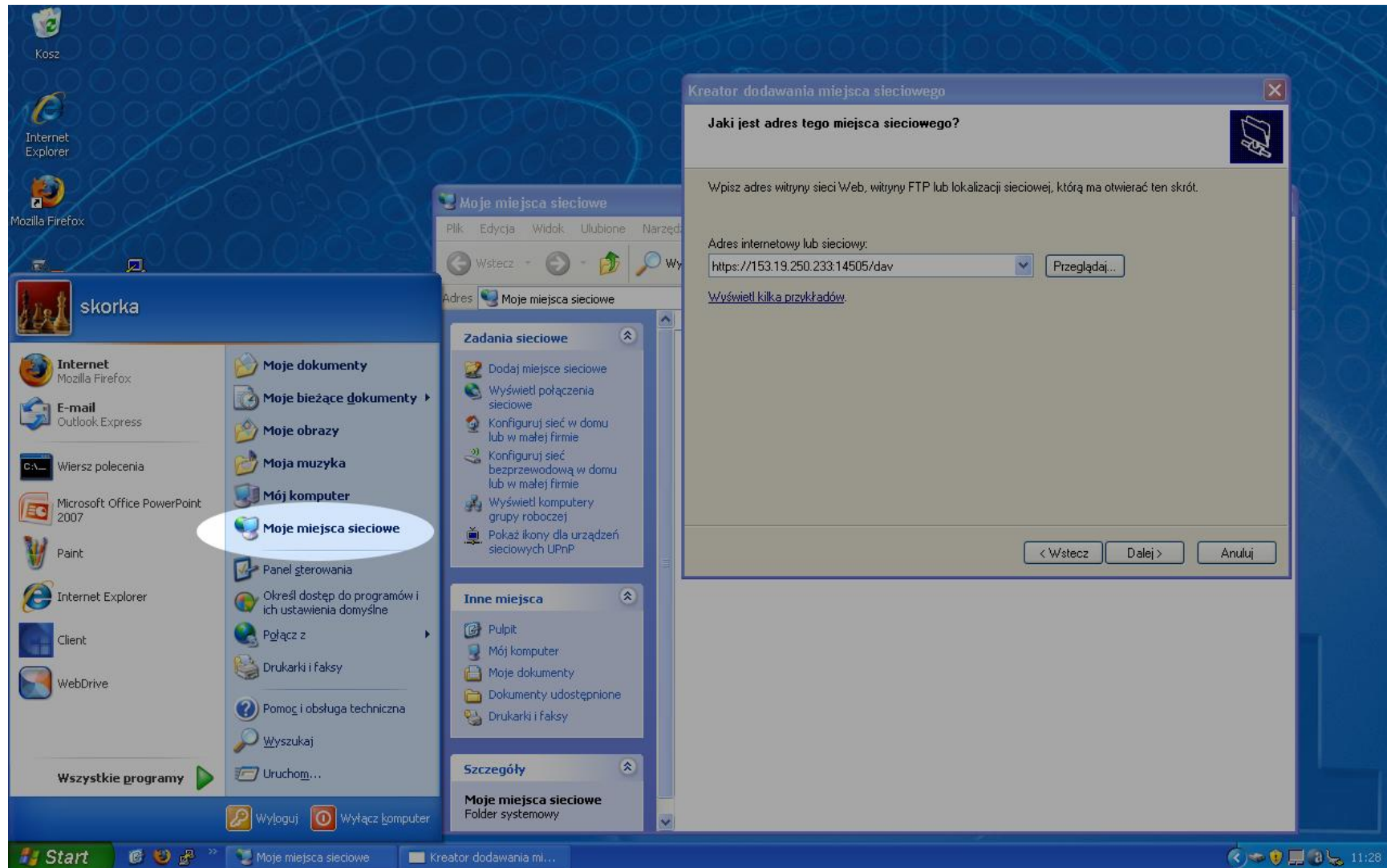
Dostęp do zasobów przez WebDAV

- “ WebDAV jest rozszerzeniem protokołu http
- “ Autoryzacja tak jak dla dostępu przez www
- “ Dostęp przez:
 - “ Przeglądarkę www (tryb tylko do odczytu)
 - “ Klienta WebDAV (zapis i odczyt)
 - “ Dysk sieciowy (*moje miejsce sieciowe*)
 - “ Emulacja dysku lokalnego (*dysk F:*)

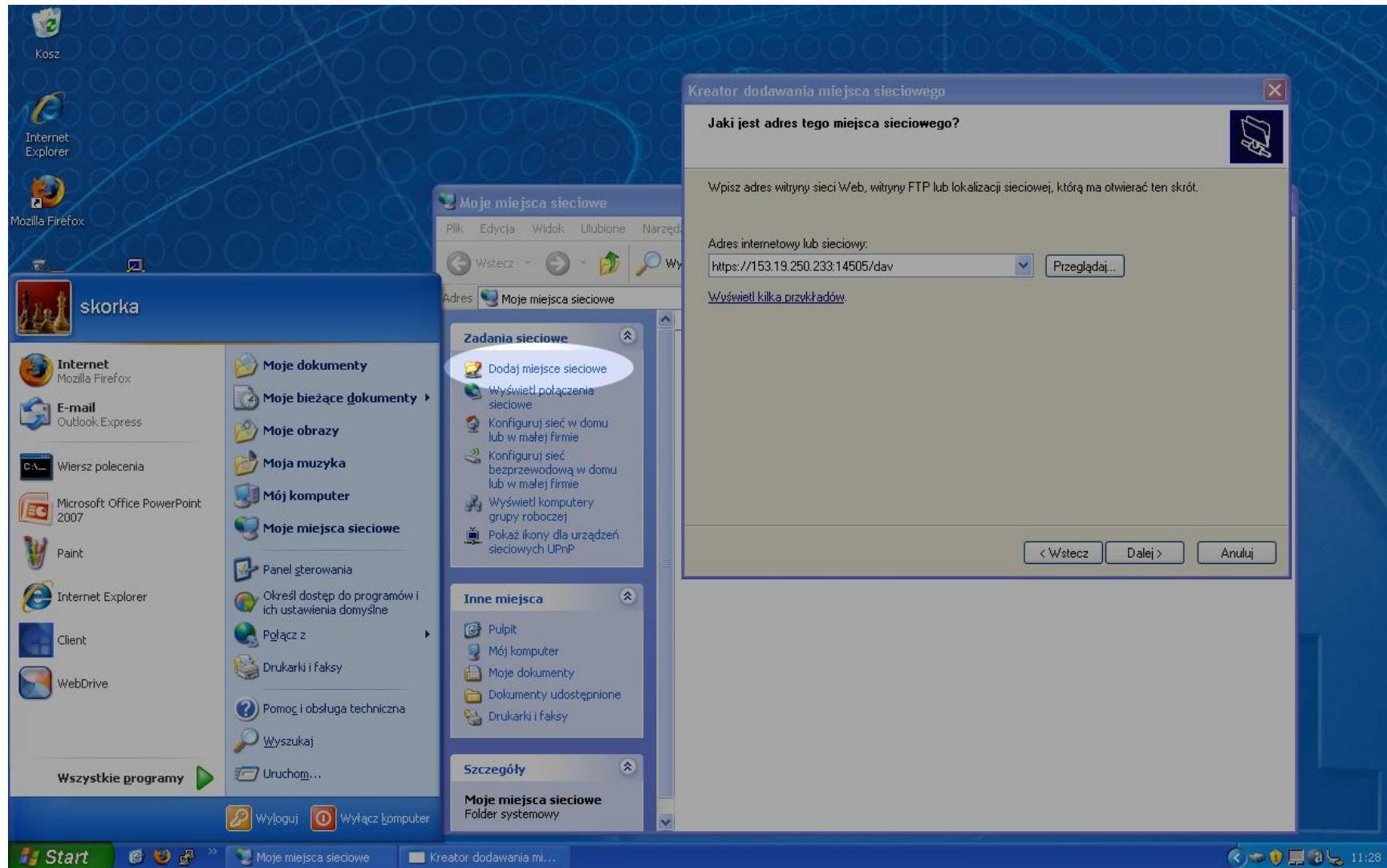
Dysk sieciowy WebDAV



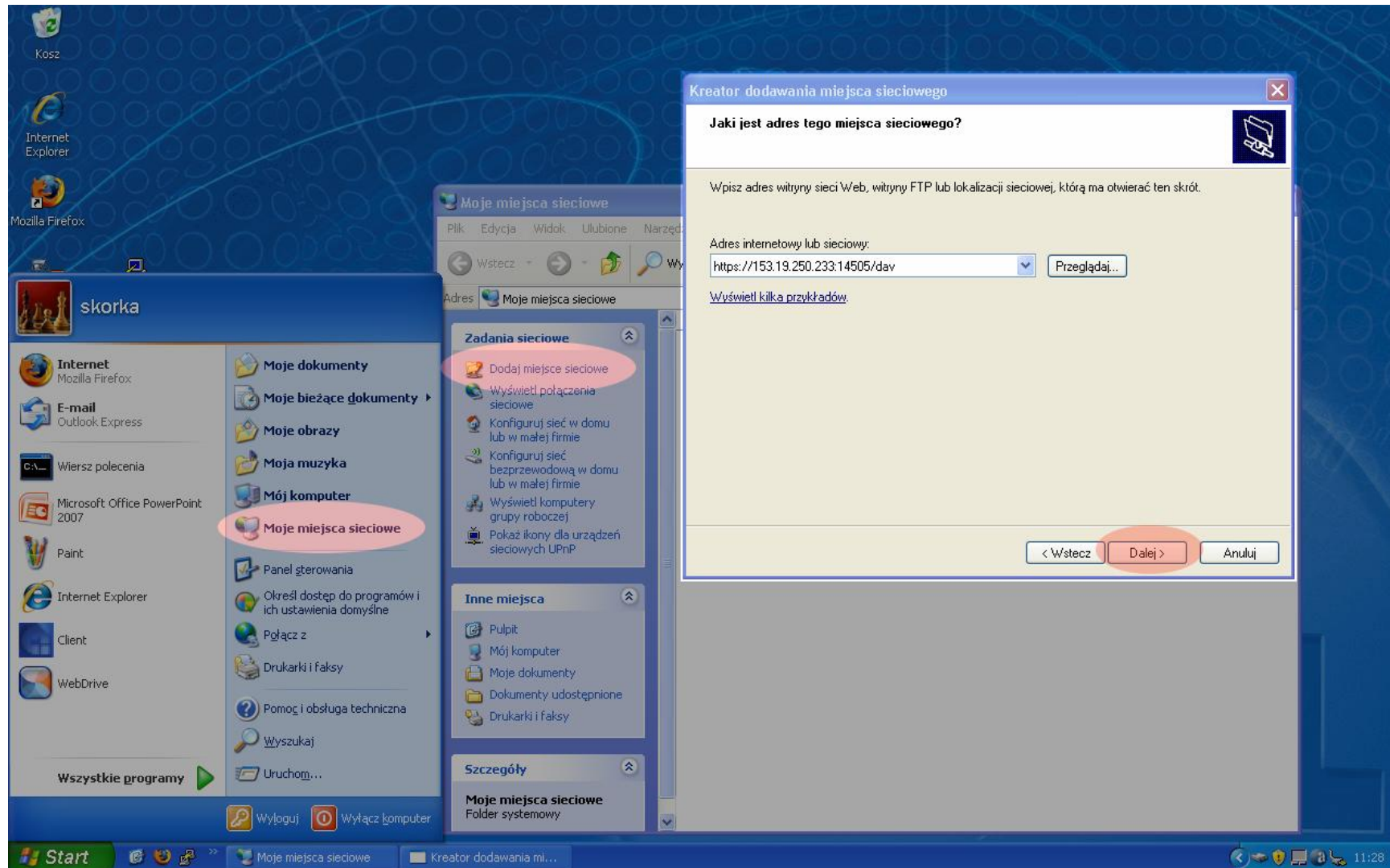
WebDAV (1)



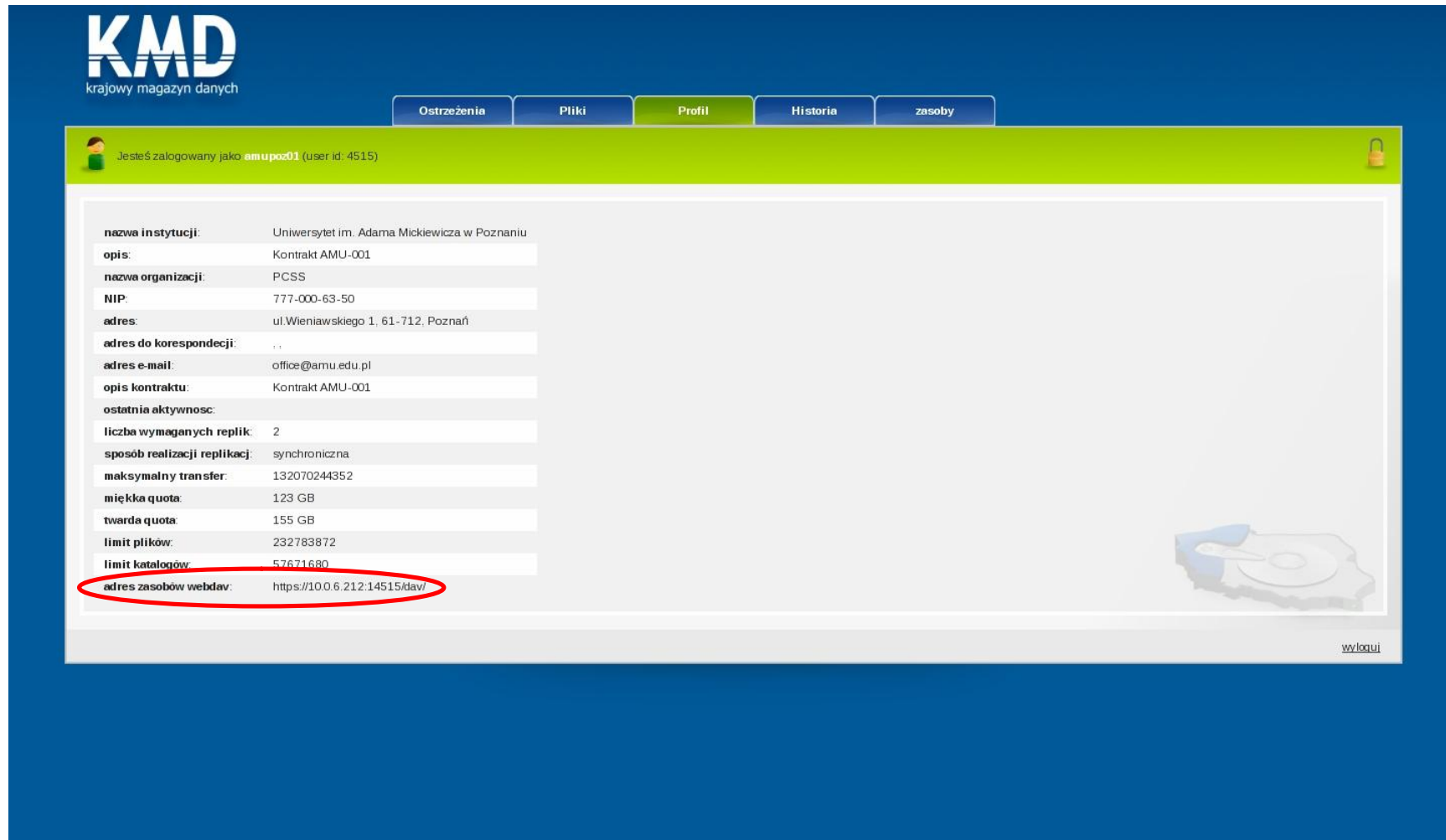
WebDAV (2)



WebDAV (3)



Adres do zasobów WebDAV



KMD
krajowy magazyn danych

Ostrzeżenia | Pliki | **Profil** | Historia | zasoby

Jesteś zalogowany jako **amupoz01** (user id: 4515)

nazwa instytucji:	Uniwersytet im. Adama Mickiewicza w Poznaniu
opis:	Kontrakt AMU-001
nazwa organizacji:	PCSS
NIP:	777-000-63-50
adres:	ul.Wieniawskiego 1, 61-712, Poznań
adres do korespondencji:	..
adres e-mail:	office@amu.edu.pl
opis kontraktu:	Kontrakt AMU-001
ostatnia aktywnosc:	
liczba wymaganych replik:	2
sposób realizacji replikacji:	synchroniczna
maksymalny transfer:	132070244352
miękką quota:	123 GB
twarda quota:	155 GB
limit plików:	232783872
limit katalogów:	57671680
adres zasobów webdav:	https://10.0.6.212:14515/dav/

w/loqui

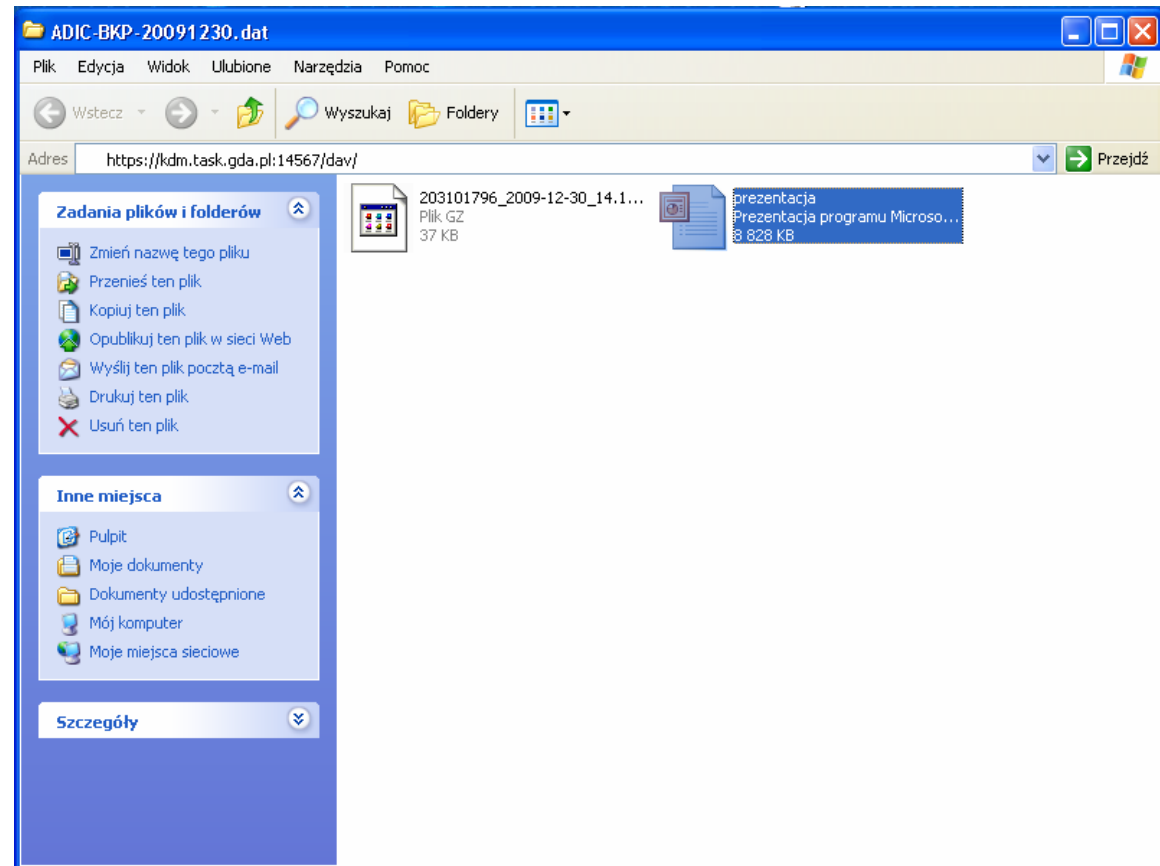
WebDAV jako zasób sieciowy

Widoczny tylko w okienku

Brak bezpośredniego dostępu z poziomu aplikacji

Mało praktyczny

Trudności w konfigurowaniu



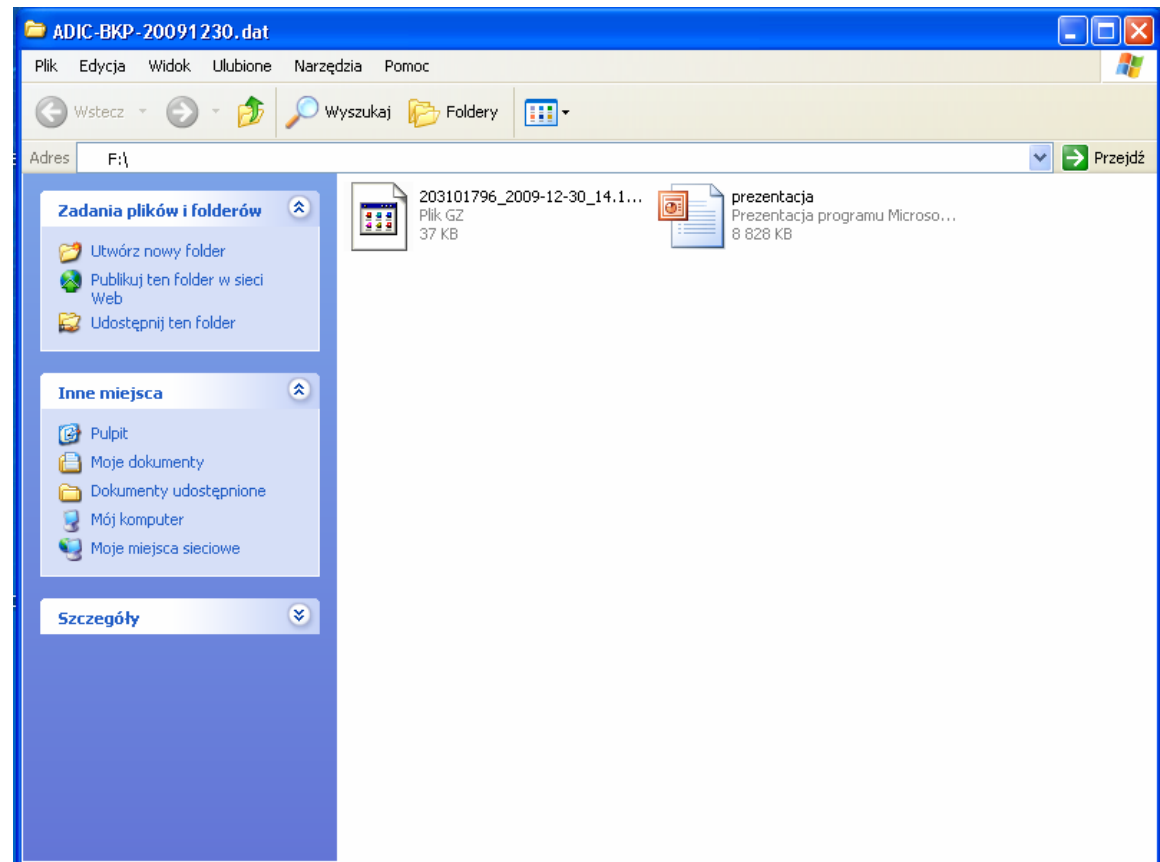
WebDAV jako dysk lokalny

Bezpośredni dostęp do danych

Niepotrzebne wsparcie dla WebDAV w aplikacjach

Bardzo praktyczny

Nie tylko WebDAV





WebDAV jako dysk - WebDrive

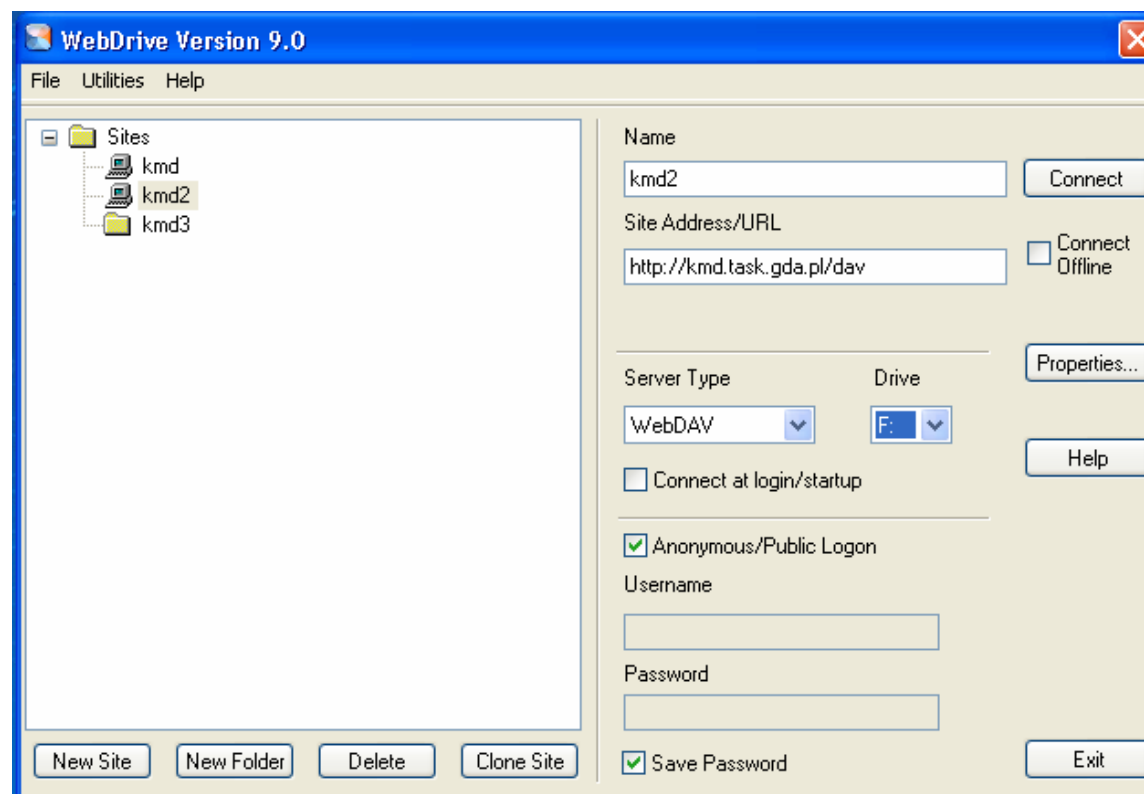
WebDrive FTP Client

łatwe zarządzanie

Optymalizacja
zasobów

Niezawodność
większa niż „Miejsca
sieciowego Windows”

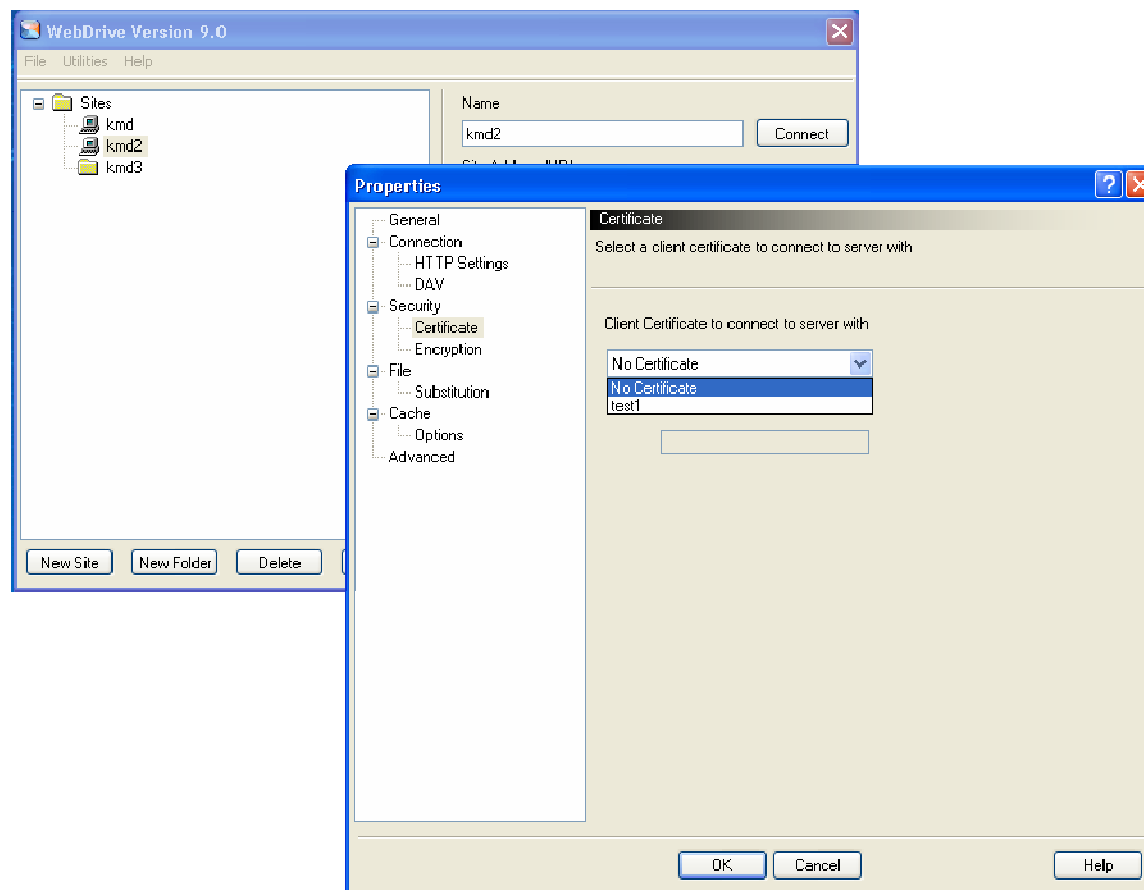
produkt komercyjny
około 200zł za licencje/rok



WebDrive FTP Client

Obsługa
certyfikatów

Możliwość
korzystania z kilku
zasobów w
jednym czasie



Podsumowanie dostępu przez http

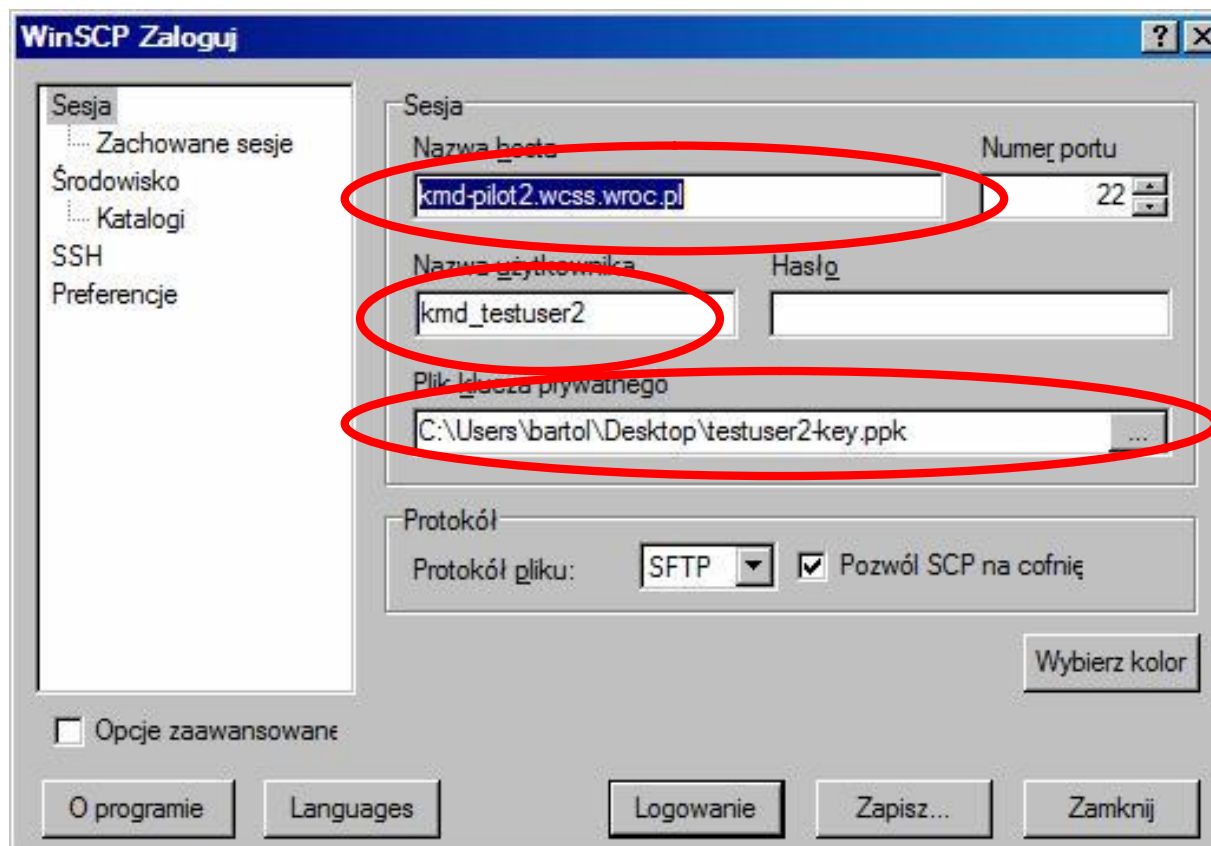
- ” Klient www
 - ” Przeglądarka www
 - ” Obsługa konta
 - ” Podgląd i edycja metadanych
- ” Klient webdav
 - ” Dysk sieciowy
 - ” Operacje na plikach
- ” Dostęp przez certyfikaty użytkownika

Dostęp przez protokół SSH

- . Dostęp po protokole SSH możliwy tylko z użyciem klucza prywatnego
- . Windows: WinSCP
 - . Darmowa aplikacja
 - . Interfejs typu „Total Commander”
- . Windows: WebDrive
 - . Komercyjna aplikacja, ta sama co dla WebDAV
- . Linux: SFTP (nie – SCP)
 - . Kopiowanie interaktywne i wsadowe
- . Linux: SSHFS
 - . Montowanie zdalnego systemu plików

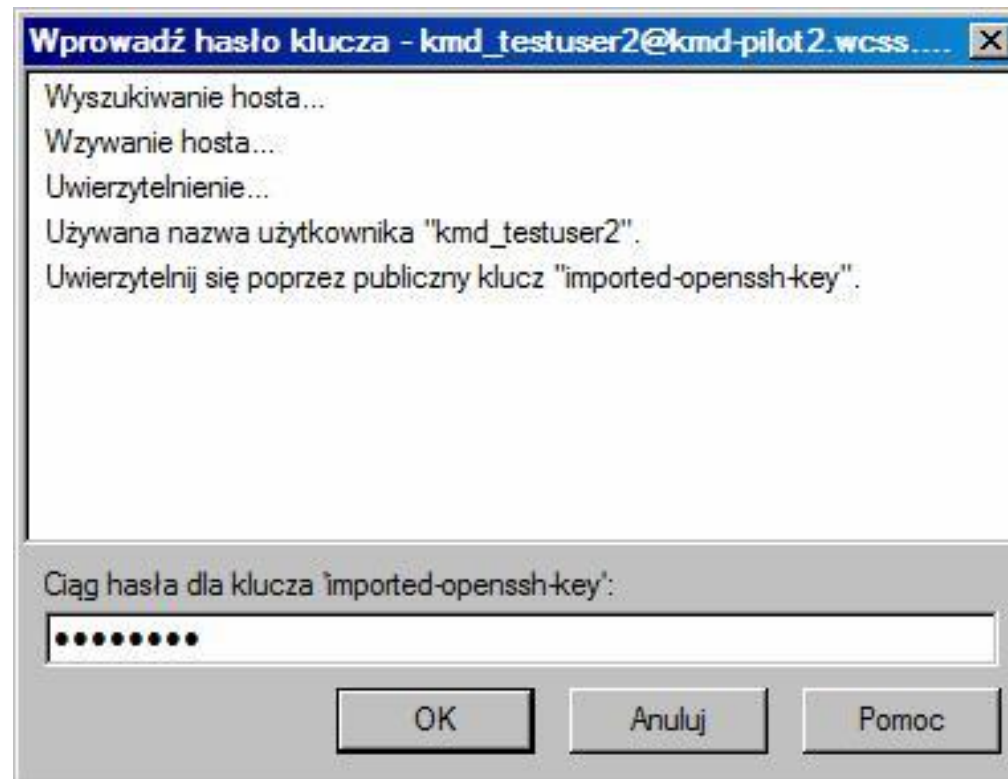
Dostęp przez protokół SSH - WinSCP

Definiowanie połączenia i wskazanie pliku z kluczem prywatnym

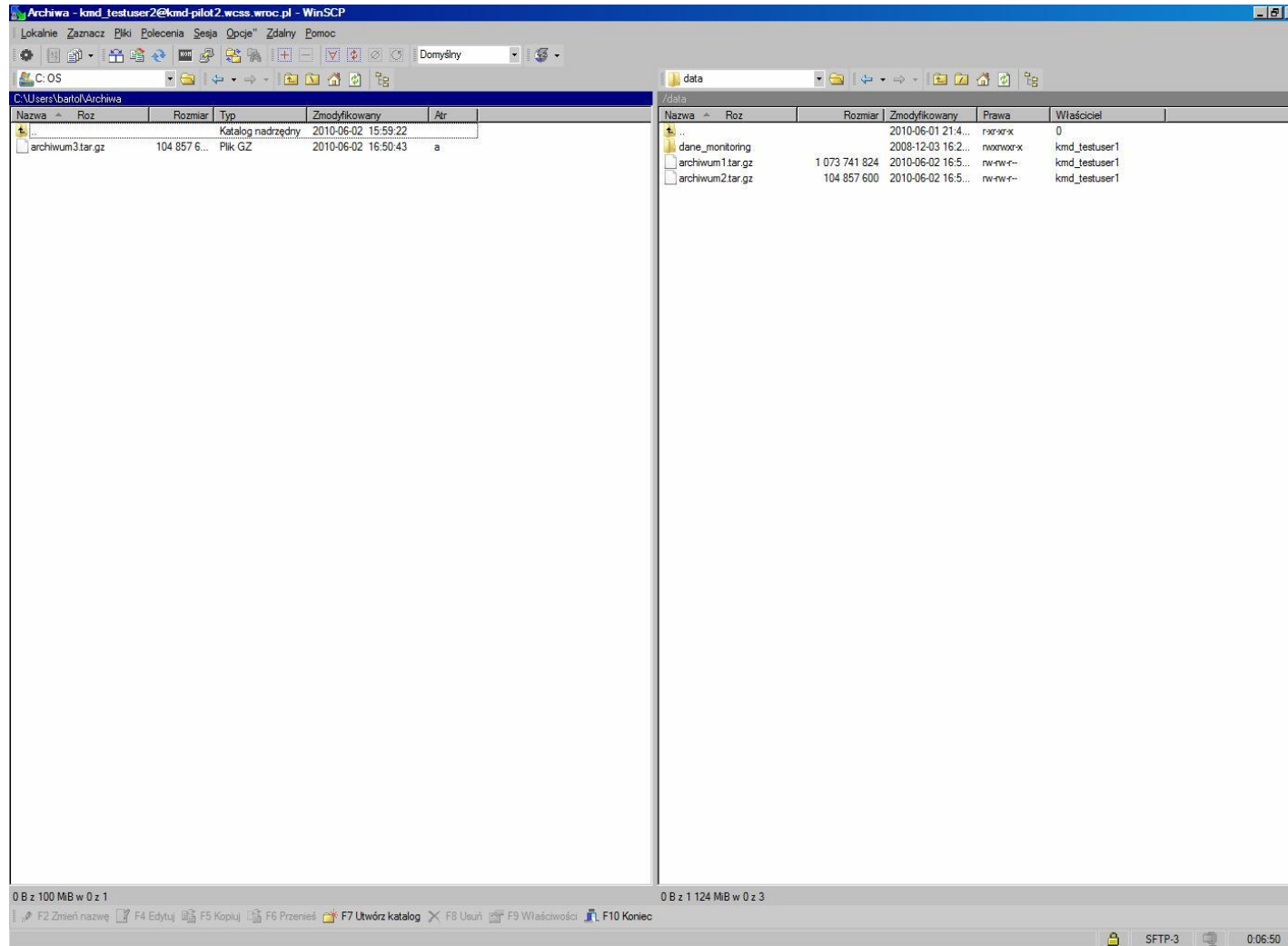


Dostęp przez protokół SSH - WinSCP

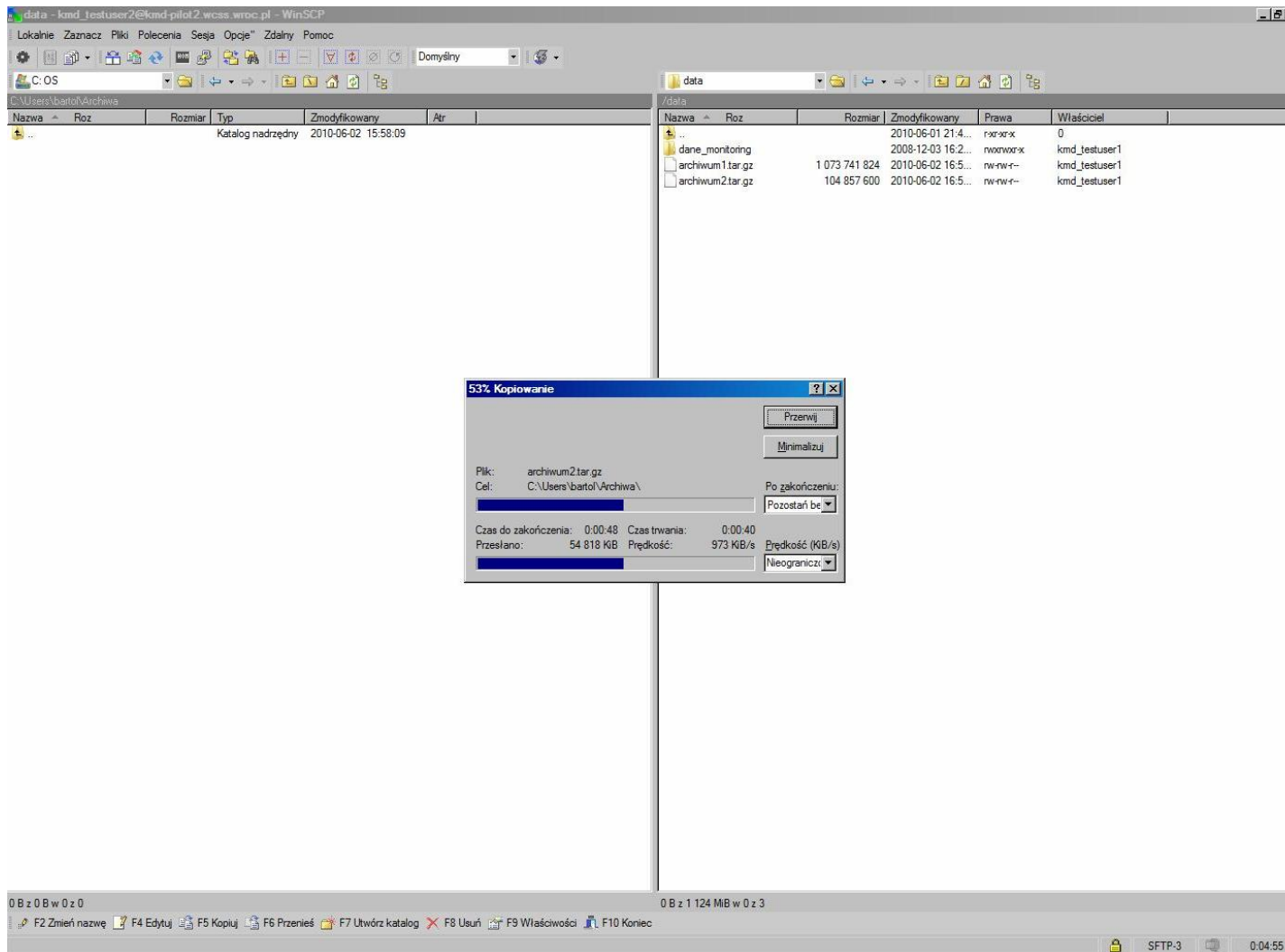
Klucz prywatny chroniony hasłem:



Dostęp przez protokół SSH - WinSCP



Dostęp przez protokół SSH - WinSCP



Dostęp przez protokół SSH - SFTP

- . Standardowy klient w systemach Linux
- . Możliwość pracy interaktywnej (FTP) jak i wsadowej (skrypty)
- . Możliwość użycia agenta SSH (ssh-agent) dla nieinteraktywnego logowania
- . Zalogowanie do zdalnego systemu i wysłanie pliku do archiwum:
 - . *sftp -b skrypt.txt kmd_testuser2@kmd-pilot2*
 - . *skrypt.txt: \$ put archiwum1.tar.gz data*
 - . *\$ Uploading archiwum1.tar.gz to data/archiwum1.tar.gz*

Dostęp przez protokół SSH - SSHFS

- . Darmowy klient pod systemy Linux
- . Umożliwia zamontowanie lokalnie zdalnego katalogu
- . Możliwość użycia agenta SSH (ssh-agent) dla nieinteraktywnego logowania
- . Zamontowanie zdalnego katalogu w lokalnym katalogu `~/platon` i skopiowanie tam pliku :
 - . `sshfs kmd_testuser2@kmd-pilot2: platon`
 - . `cp archiwum1.tar.gz platon/data`

Dostęp przez protokół GridFTP

- . Dostęp z poziomu systemów gridowych działających w oparciu o system Globus Toolkit
- . Uwierzytelnianie dzięki certyfikatom
- . Wygenerowanie tymczasowego certyfikatu dostępu oraz skopiowanie pliku:
 - . *grid-proxy-init -cert amupoz01.p12*
 - . *globus-url-copy file:///archiwum1.tar.gz gsiftp://kmd-pilot2/~data/*

Gdzie zamówi usług ?

“ Białystok - Politechnika Białostocka,
“ Centrum Komputerowych Sieni Rozległych
“ platon-u4-req@biaman.pl
“

“ Częstochowa - Politechnika Częstochowska,
“ Instytut Informatyki Teoretycznej i
Stosowanej, PCz
“ platon-u4-req@icis.pcz.pl
“

“ Gdańsk - Politechnika Gdańska,
“ Centrum Informatyczne Trójmiejskiej
Akademickiej Sieni Komputerowej TASK
“ platon-u4-req@task.gda.pl
“

“ Kielce – Politechnika Świętokrzyska
“ platon-u4-req@tu.kielce.pl



Gdzie zamówi usług ?

” Kraków ó Akademia Górniczo-Hutnicza,

” Akademickie Centrum Komputerowe CYFRONET AGH

” platon-u4-req@cyfronet.pl

”

” Lublin - Uniwersytet Marii Curie-Skłodowskiej w Lublinie,

” Lub MAN UMCS

” platon-u4-req@umcs.lublin.pl

”

” / ód - Politechnika/ ódzka,

” Centrum Komputerowe P/ , Miejska Sie Komputerowa LOD

” platon-u4-req@man.lodz.pl

” Kraków ó Akademia Górniczo-Hutnicza,

” Akademickie Centrum Komputerowe CYFRONET AGH

” platon-u4-req@cyfronet.pl

”

” Lublin - Uniwersytet Marii Curie-Skłodowskiej w Lublinie,

” Lub MAN UMCS

” platon-u4-req@umcs.lublin.pl

”

” / ód - Politechnika/ ódzka,

” Centrum Komputerowe P/ , Miejska Sie Komputerowa LOD

” platon-u4-req@man.lodz.pl

Kroki rejestracyjne

- ” Wysłanie zgłoszenia na adres jednego z o rodków bior cych udział w projekcie
- ” Wypełnienie otrzymanego w odpowiedzi formularza rejestracji usługi i odesłanie go na adres kontaktowy
- ” Po poprawnym zweryfikowaniu formularza otrzymujemy informację z pro b o dostarczenie swojego certyfikatu X509 lub odebranie certyfikatu wygenerowanego przez CA usługi archiwizacji
- ” Po zakończeniu wszystkich powy szych kroków otrzymujemy informację potwierdzając proces zakończenia rejestracji i aktywacji usługi.

Dane rejestracyjne

- ” Dane **identyfikuj ce instytucj** z jakiej pochodzi u ytkownik:
dane teleadresowe
- ” Dane **identyfikuj ce u ytkownika** ko cowego:
dane teleadresowe,
certyfikat u ytkownika, certyfikat CA u ytkownika
- ” Dane okre laj ce **profil** zamawianej usługi:
wielko zasobów,
liczba replik,
dost pno danych itp.

Certyfikaty u ytkowników

- “ U ytkownicy korzystaj cy z usŁugi musz posiada **certyfikat X509**
- “ **Certyfikat u ytkownika mo e zosta wygenerowany i podpisany** przez CA usŁugi archiwizacji w trakcie procedury rejestracyjnej
- “ **U ytkownik mo e dostarczy swój certyfikat** podpisany przez inne CA w trakcie procedury rejestracyjnej
- “ (ale wtedy konieczne jest dostarczenie b d wskazanie miejsca sk d mo na pobra certyfikat CA podpisuj cego certyfikat u ytkownika)

Podsumowanie

- ” Oprogramowanie KMD i Usługa Powszechnej Archiwizacji daje użytkownikom dostęp do skalowalnej i rozproszonej infrastruktury opartej na nowoczesnej technologii ónieosi galnej dla większości instytucji
- ” System został zaprojektowany tak, aby spełniał wymagania użytkowników w zakresie:
 - ” Bezpieczeństwa danych
 - ” Wysokiej trwałości danych
 - ” Niezawodności
 - ” Prosty użytkowania
- ” System jest innowacyjny względem istniejących rozwiązań

Podsumowanie

- ” Usługa dostarcza użytkownikom rozmaite interfejsy dostępu do danych składowanych w wirtualnym systemie plików oraz umożliwia automatyzację i optymalizację procesu wykonywania kopii zapasowych i archiwalnych poprzez wykorzystanie aplikacji klienta opracowanego w projekcie KMD.
- ” Wykorzystanie usług systemu zwalnia użytkowników z konieczności desygnowania znacznych zasobów na potrzeby zabezpieczenia i archiwizacji danych.
- ” Interfejsy i funkcjonalność systemu pozwala na efektywne wykorzystanie usług na potrzeby zabezpieczenia i archiwizacji danych bibliotek naukowych.

Dzi kujemy za uwag !

