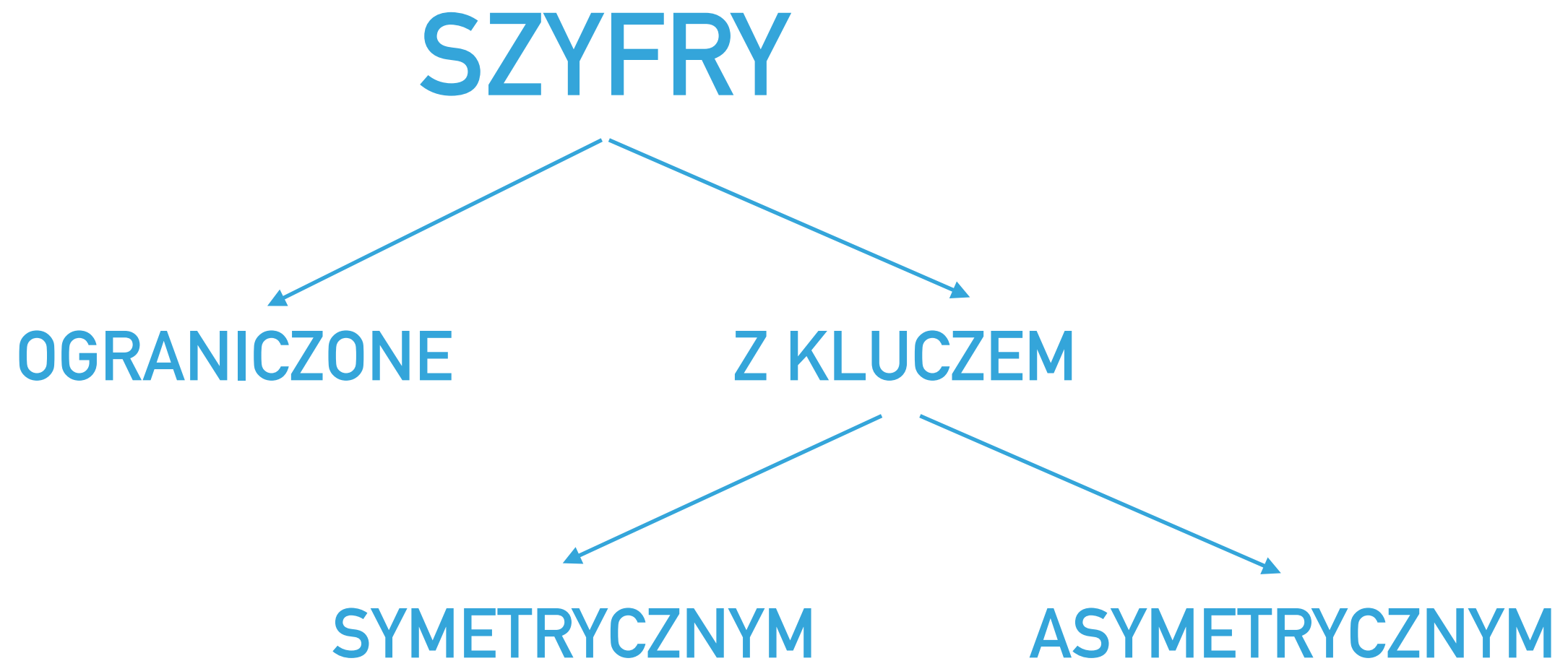


ADMINISTRACJA I BEZPIECZEŃSTWO SYSTEMÓW KOMPUTEROWYCH

UWIERZYTELNIANIE KLIENTA
APLIKACJI WEBOWYCH ZA POMOCĄ
CERTYFIKATÓW

SZYFROWANIE



CERTYFIKATY

- ▶ Certyfikat klucza publicznego
 - ▶ Klucz publiczny
 - ▶ Opis tożsamości
 - ▶ Podpis zaufanej instytucji (Certificate Authority)

CERTYFIKATY

- ▶ Certyfikat samopodpisany (self-signed certificate)
- ▶ Standard X.509
- ▶ Uwierzytelnianie:
 - ▶ Serwera
 - ▶ Klienta

SSL I TLS

- ▶ Protokoły kryptograficzne
- ▶ Powszechnie przyjęte jako standard
- ▶ Bezpieczeństwo, poufność, integralność danych
- ▶ Oparte na:
 - ▶ Szyfrowaniu z kluczem
 - ▶ Certyfikatach X.509

IMPLEMENTACJA

UTWORZENIE CERTYFIKATÓW

- ▶ Utworzenie certyfikatu głównego
- ▶ Utworzenie certyfikatu klienta

STWORZENIE CERTYFIKATU GŁÓWNEGO

- ▶ 1. Wygenerowanie klucza prywatnego Instytucji uwierzytelniającej
- ▶ 2. Stworzenie prośby o podpisanie certyfikatu
- ▶ 3. Samopodpisanie certyfikatu
- ▶ 4. Stworzenie pary certyfikatu i klucza publicznego

STWORZENIE CERTYFIKATU GŁÓWNEGO

- ▶ `openssl genrsa -out SabatKeyCA.key 2048`
- ▶ `Openssl req -new -nodes -key SabatKeyCA.key -out SabatRequestCA.csr`
- ▶ `openssl x509 -req -trustout -days 365 -in SabatRequestCA.csr -signkey SabatKeyCA.key -out SabatCertCA.crt`
- ▶ `openssl pkcs12 -export -in SabatCertCA.crt -inkey SabatKeyCA.key -out SabatPairCA.pfx`

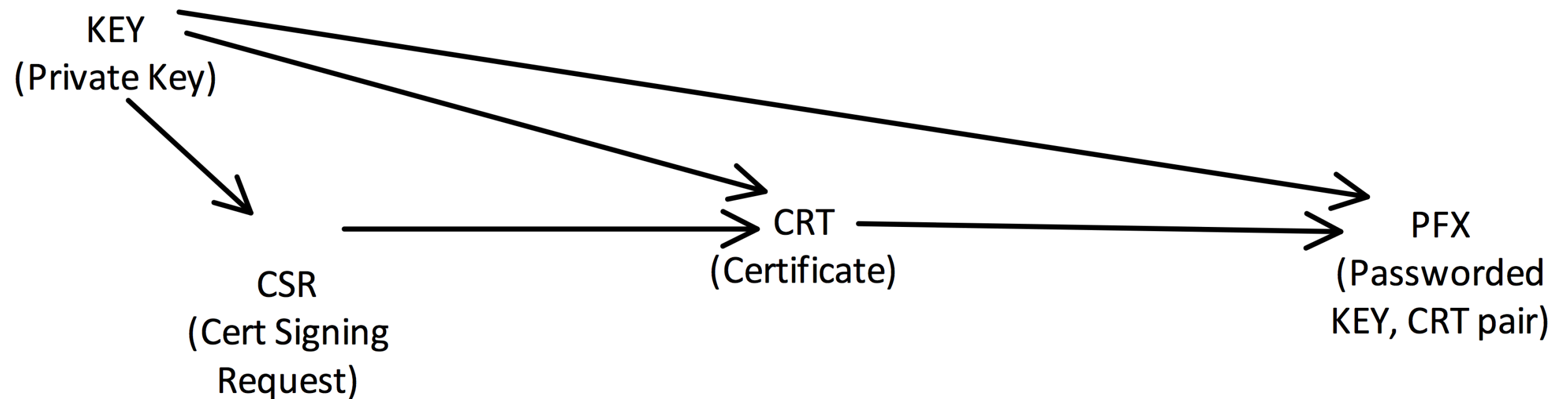
STWORZENIE CERTYFIKATU KLIENTA

- ▶ 1. Wygenerowanie klucza prywatnego klienta
- ▶ 2. Stworzenie prośby o podpisanie certyfikatu
- ▶ 3. Podpisanie certyfikatu klienta za pomocą certyfikatu głównego i klucza
- ▶ 4. Stworzenie pary certyfikatu i klucza publicznego klienta

STWORZENIE CERTYFIKATU KLIENTA

- ▶ `openssl genrsa -out sabattestclientcert.key 2048`
- ▶ `openssl req -new -nodes -key sabattestclientcert.key -out sabattestclientcert.csr`
- ▶ `openssl x509 -req -days 365 -in sabattestclientcert.csr -CA SabatCertCA.crt -CAkey SabatKeyCA.key -set_serial 01 -out sabattestclientcert.crt`
- ▶ `openssl pkcs12 -export -in sabattestclientcert.crt -inkey sabattestclientcert.key -out sabattestclientcert.pfx`

TWORZENIE PLIKÓW CERTYFIKATÓW



IMPORT CERTYFIKATÓW

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

FileActionViewFavoritesWindowHelp

←→📁📄🔄📧?

Console Root

▼Certificates - Current User

▼Personal

Certificates

▼Trusted Root Certification Authorities

Certificates

>Enterprise Trust

>Intermediate Certification Authorities

>Active Directory User Object

>Trusted Publishers

>Untrusted Certificates

>Third-Party Root Certification Authorit

>Trusted People

>Client Authentication Issuers

>Local NonRemovable Certificates

>MSIEHistoryJournal

>Certificate Enrollment Requests

>Smart Card Trusted Roots

>Certificates (Local Computer)

Issued To

DS\cxvr47

sabattestclientcert

Wojtek Sabat

Issued By

DS\cxvr47

Wojciech Sabat

Wojtek Sabat

Actions

Certificates

More Actions

STRUKTURA APLIKACJI

Admibesyko Strona główna API Dane ściśle tajne

Administracja i Bezpieczeństwo Systemów Komputerowych

Projekt przedstawiający wykorzystanie certyfikatu klienta do uwierzytelnienia w aplikacji webowej.

Te dane są jawne i mogą być widziane przez każdego

Politechnika Krakowska

Politechnika Krakowska »

Certyfikaty

Certyfikaty SSL/TLS według Wikipedii

Wikipedia »

Szyfrowanie asymetryczne według Wikipedi

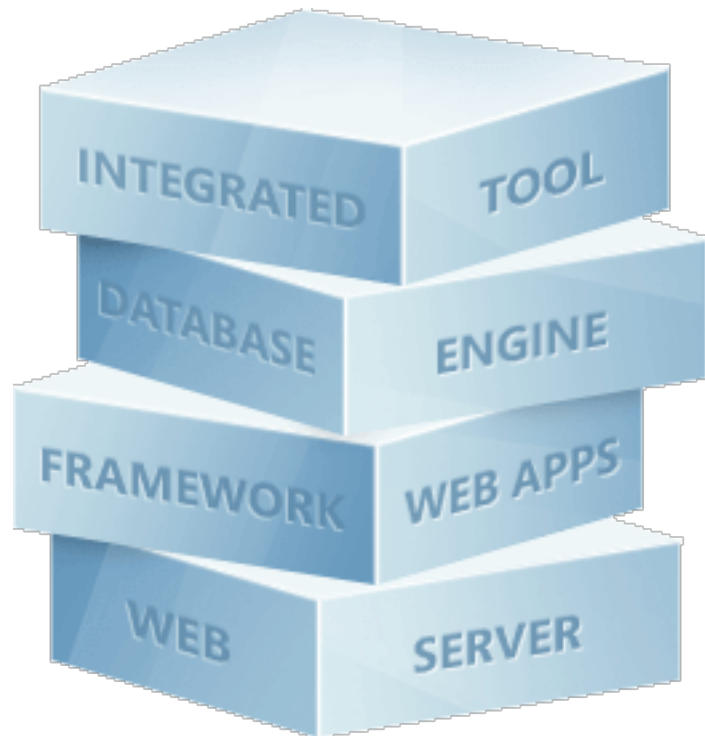
Szyfrowanie klucza publicznego.

Wikipedia »

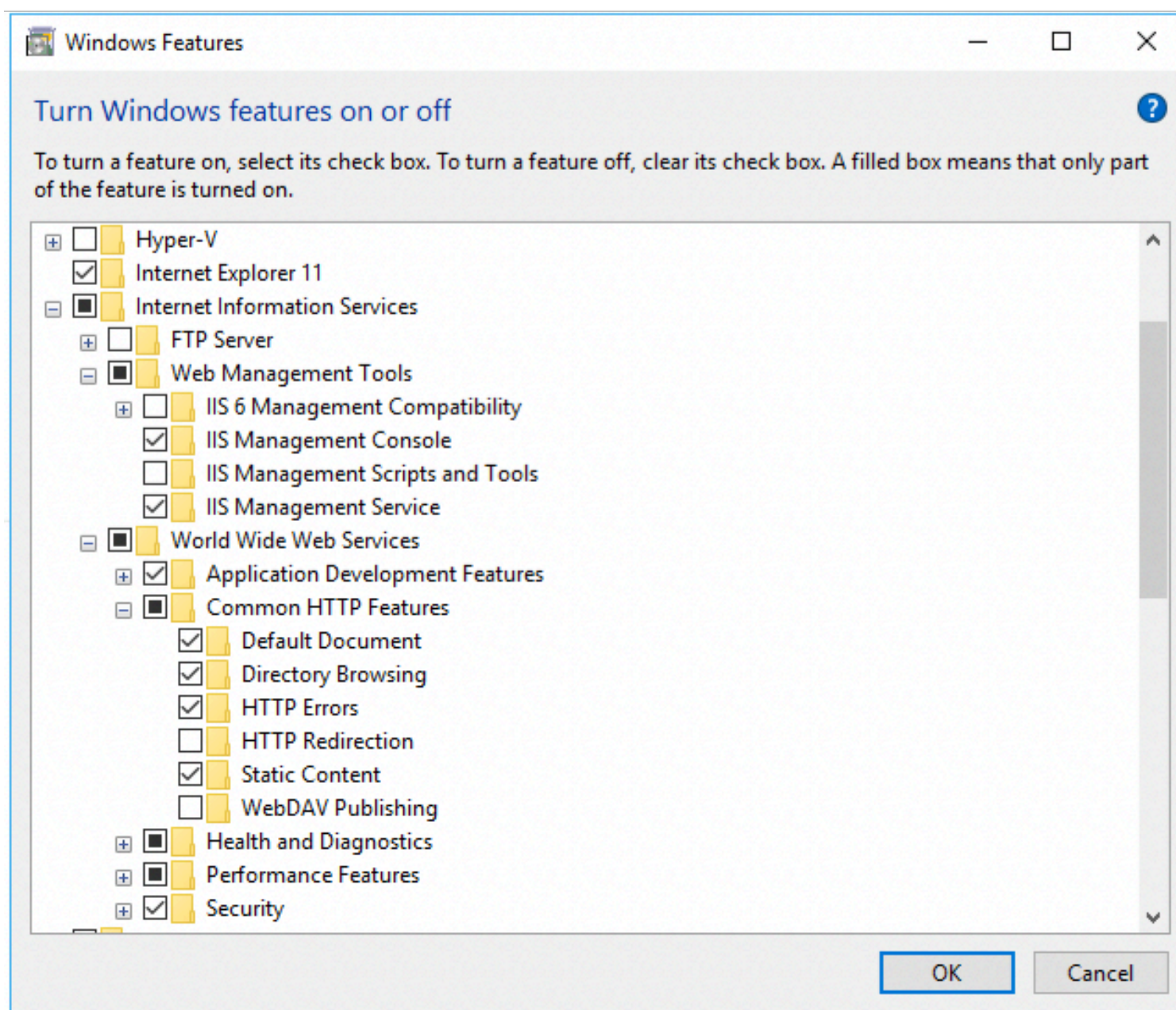
STRUKTURA APLIKACJI

sabattestsite.local/StudentGrades				
Admibesylko Strona główna API Dane ściśle tajne				
Ściśle tajne oceny końcowe				
Name	Surname	University	Group	Final Grade
Jan	Kowalski	Politechnika Krakowska	13k5	4
Maciej	Nowak	Uniwersytet Jagielloński	12k8	3
Zbigniew	Zawisza	Politechnika Krakowska	13k4	2,5
Wioletta	Kwiecień	Uniwersytet Jagielloński	13k2	4,75
Zygmunt	Noszczyński	Akademia Górniczo Hutnicza	11k1	4
Monika	Kubowicz	Politechnika Krakowska	11k4	3
Karolina	Curuś	Uniwersytet Jagielloński	13k5	2
Marcin	Miśkowiec	Politechnika Krakowska	11k3	3,5
Abelard	Stokłosa	Akademia Górniczo Hutnicza	13k4	4
Anastazja	Kamiński	Politechnika Krakowska	13k4	4,98
Jarosław	Lem	Politechnika Krakowska	12k5	3
Eugeniusz	Szymański	Akademia Górniczo Hutnicza	13k1	4,4
© 2017 - Wojciech Sabat Grupa 13k5				

PROBLEM Z SERWEREM IIS



KONFIGURACJA IIS



KONFIGURACJA IIS

The screenshot shows the 'Add Website' dialog box in IIS Manager. The dialog is titled 'Add Website' and has a question mark icon and a close button (X) in the top right corner. It contains several sections for configuring a new website.

Site name: sabattestsite.local

Application pool: sabattestsite.local (with a 'Select...' button)

Content Directory

Physical path: C:\AdmibeszykoCerts\ClientCertAuthWebApi\ClientCert\ (with a browse button '...')

Pass-through authentication

Connect as... **Test Settings...**

Binding

Type: https (dropdown menu)

IP address: All Unassigned (dropdown menu)

Port: 443

Host name: sabattestsite.local

☐ Require Server Name Indication

SSL certificate: sabattestsite.local (dropdown menu) **Select...** **View...**

☒ Start Website immediately

OK **Cancel**

KONFIGURACJA IIS



SSL Settings

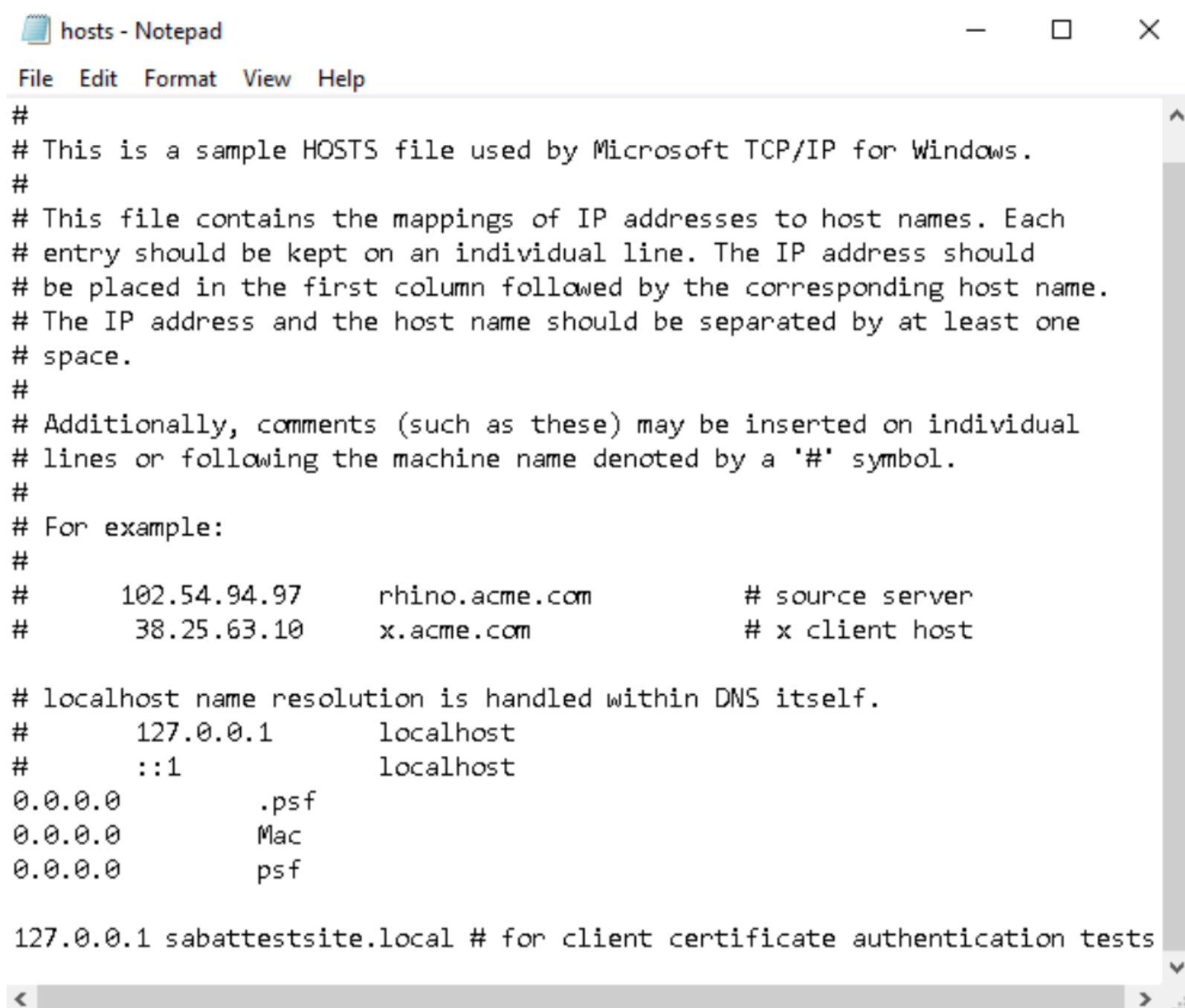
This page lets you modify the SSL settings for the content of a website or application.

☒ Require SSL

Client certificates:

- ☐ Ignore
- ☒ Accept
- ☐ Require

KONFIGURACJA IIS



```
#  
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.  
#  
# This file contains the mappings of IP addresses to host names. Each  
# entry should be kept on an individual line. The IP address should  
# be placed in the first column followed by the corresponding host name.  
# The IP address and the host name should be separated by at least one  
# space.  
#  
# Additionally, comments (such as these) may be inserted on individual  
# lines or following the machine name denoted by a '#' symbol.  
#  
# For example:  
#  
#       102.54.94.97       rhino.acme.com           # source server  
#       38.25.63.10       x.acme.com               # x client host  
  
# localhost name resolution is handled within DNS itself.  
#       127.0.0.1         localhost  
#       ::1               localhost  
0.0.0.0       .psf  
0.0.0.0       Mac  
0.0.0.0       psf  
  
127.0.0.1 sabattestsite.local # for client certificate authentication tests
```


KONFIGURACJA IIS

ClientCertAuthWebApi X StudentGradesController.cs

Application

Build

Web

Package/Publish Web

Package/Publish SQL

Build Events

Resources

Settings

Reference Paths

Signing

Code Analysis

Configuration: N/A

Platform: N/A

Start Action

☒ Current Page

☐ Specific Page

☐ Start external program

☐ Start URL

☐ Don't open a page. Wait for a request from an external application.

Command line arguments

Working directory

Servers

☒ Apply server settings to all users (store in project file)

Local IIS

Project Url

https://sabattestsite.local/

Create Virtual Directory

☐ Override application root URL

https://sabattestsite.local/

Debuggers

☒ ASP.NET

☐ Native Code

☐ SQL Server

☐ Silverlight

☒ Enable Edit and Continue

OWIN I KATANA



Microsoft.Owin.Host.SystemWeb by Microsoft

✓ v3.1.0

OWIN server that enables OWIN-based applications to run on IIS using the ASP.NET request pipeline.



Microsoft.Owin.Security by Microsoft

✓ v3.1.0

Common types which are shared by the various authentication middleware components.

```
0 references | Wojciech Sabat, 2 days ago | 1 author, 1 change
public class Startup
{
    0 references | Wojciech Sabat, 2 days ago | 1 author, 1 change | 0 exceptions
    public void Configuration(IApplicationBuilder appBuilder)
    {
    }
}
```

IMPLEMENTACJA KLAS

```
public class ClientCertificateAuthenticationOptions : AuthenticationOptions
{
    1 reference | Wojciech Sabat, 2 days ago | 1 author, 1 change | 0 exceptions
    public ClientCertificateAuthenticationOptions() : base("X.509")
    { }
}
```

IMPLEMENTACJA KLAS

```
public class ClientCertificateAuthenticationHandler : AuthenticationHandler<ClientCertificateAuthenticationOptions>
{
    private readonly IClientCertificateValidator _clientCertificateValidator;
    private readonly string _owinClientCertKey = "ssl.ClientCertificate";

    1 reference | Wojciech Sabat, 14 minutes ago | 1 author, 2 changes | 0 exceptions
    public ClientCertificateAuthenticationHandler(IClientCertificateValidator clientCertificateValidator)...

    0 references | Wojciech Sabat, 14 minutes ago | 1 author, 2 changes | 0 exceptions
    protected override async Task<AuthenticationTicket> AuthenticateCoreAsync()...

    1 reference | Wojciech Sabat, 2 days ago | 1 author, 1 change | 0 exceptions
    private ClientCertificateValidationResult ValidateCertificate(IDictionary<string, object> owinEnvironment)...
}
```


IMPLEMENTACJA KLAS

```
9 references | Wojciech Sabat, 2 days ago | 1 author, 1 change
public class ClientCertificateValidationResult
{
    private readonly bool _isCertificateValid;
    private readonly IEnumerable<string> _validationExceptions;

    2 references | Wojciech Sabat, 2 days ago | 1 author, 1 change | 0 exceptions
    public ClientCertificateValidationResult(bool isCertificateValid)...

    1 reference | Wojciech Sabat, 2 days ago | 1 author, 1 change | 0 exceptions
    public void AddValidationExceptions(IEnumerable<string> validationExceptions)...

    1 reference | Wojciech Sabat, 2 days ago | 1 author, 1 change | 0 exceptions
    public void AddValidationException(string validationException)...

    1 reference | 0 changes | 0 authors, 0 changes | 0 exceptions
    public bool IsCertificateValid => _isCertificateValid;
}
```

IMPLEMENTACJA KLAS

```
public class ClientCertificateValidator : IClientCertificateValidator
{
    2 references | 0 changes | 0 authors, 0 changes | 0 exceptions
    public ClientCertificateValidationResult Validate(X509Certificate2 certificate)
    {
        var isValid = false;
        var exceptions = new List<string>();
        try
        {
            var chain = new X509Chain();
            var chainPolicy = new X509ChainPolicy...;
            chain.ChainPolicy = chainPolicy;
            if (chain.Build(certificate))
                isValid = true;
            else
                foreach (X509ChainElement chainElement in chain.ChainElements)
                {
                    foreach (X509ChainStatus chainStatus in chainElement.ChainElementStatus)
                    {
                        exceptions.Add(chainStatus.StatusInformation);
                    }
                }
        }
        catch (Exception ex)
        {
            exceptions.Add(ex.Message);
        }
        var result = new ClientCertificateValidationResult(isValid);
        result.AddValidationExceptions(exceptions);
        return result;
    }
}
```

IMPLEMENTACJA KLAS

```
public class Startup
{
    0 references | Wojciech Sabat, 45 minutes ago | 1 author, 2 changes | 0 exceptions
    public void Configuration(IApplicationBuilder appBuilder)
    {
        appBuilder.UseClientCertificateAuthentication(new ClientCertificateValidator());
    }
}
```

IMPLEMENTACJA KLAS

```
[Authorize]
0 references | 0 changes | 0 authors, 0 changes
public class StudentGradesController : Controller
{
    private StudentRepository _repository = new StudentRepository();

    0 references | 0 changes | 0 authors, 0 changes | 0 requests | 0 exceptions
    public ActionResult Index()
    {
        var students = _repository.GetAll();
        return View(students);
    }
}
```

DZIĘKUJĘ ZA UWAGĘ

WOJCIECH SABAT

GRUPA 13K5