

Sprawozdanie 2 Ochrona Systemów Operacyjnych

Jonatan Kasperczak
07.04.2022
Cyberbezpieczeństwo 2022

OPENSSL



Zadania do realizacji na dowolnym systemie Linux:



1. Utworzenie przy użyciu narzędzia OpenSSL lokalnego centrum certyfikacji (ang. CA).
2. Wygenerowanie wniosku o podpisanie certyfikatu osobistego (ang. CSR)
3. Podpisanie tego wniosku i wygenerowanie osobistego certyfikatu klucza publicznego zawierającego:
 - a) Własne imię nazwisko
 - b) Adres e-mail poczty studenckiej
 - c) Atrybuty umożliwiające podpisywanie poczty
 - d) Atrybuty umożliwiające podpisywanie komunikacji SSL/TLS jako klient

W załącznikach znajdują się

Certyfikat osobisty w formatach PEM oraz tekstowym

Certyfikat CA w formatach PEM oraz tekstowym

Wynik weryfikacji certyfikatu osobistego certyfikatem CA

Zadanie 1

#Generate CA key and CA certificate

```
openssl req -x509 -newkey rsa:4096 -days 3650 -keyout ca-key.pem -out ca-cert.pem -sha256 -subj  
"/C=PL/ST=DOL/L=Włr/O=PWłr/OU=WIT/CN=Jonatan_Kasperczak/emailAddress=259418@student.pwr.edu.  
pl"
```

Zadanie 2

#Generate private sign request with attributes

```
openssl req -newkey rsa:4096 -addext "extendedKeyUsage = emailProtection,clientAuth" -keyform PEM  
-keyout server-key.pem -out server-req.csr -outform PEM -sha256 -subj  
"/C=EN/ST=ZS/L=ZS/O=Włr/OU=/CN=Kasperczak/emailAddress=259418"
```

Zadanie 3

#Sign certificate

```
openssl x509 -req -days 365 -in server-req.csr -CA ca-cert.pem -CAkey ca-key.pem -CAcreateserial -out  
server-cert.pem -sha256
```

#Convert ca to ca.txt

```
openssl x509 -in ca_cert.pem -noout -text > ca_cert.txt
```

#Convert sign-request to txt

```
openssl req -noout -text -in server-req.csr > req_csr.txt
```

#Convert signed certificate to txt

```
openssl x509 -in server-cert.pem -noout -text > cert_pem.txt
```

#Verify

```
openssl verify -CAfile ca-cert.pem server-cert.pem
```