Ćwiczenie 09

**Certyfikaty cyfrowe X.509**

Celem ćwiczenia jest zapoznanie się z procedurą tworzenia certyfikatów podpisu cyfrowego   
w standardzie X.509 z wykorzystaniem:

(1) aplikacji CrypTool i aplikacji Kleopatra,

(2) serwera certyfikatów.

1. Pobierz aplikację CrypTool 1 w wersji CT 1.4.4x (lub nowszej, ale nie wersję 2.x): [CrypTool 1 - CrypTool Portal](https://www.cryptool.org/en/ct1/)
2. Zainstaluj aplikację.
3. Uruchom aplikację; na ekranie pojawi się plik startingexample-pl.txt.
4. Wygeneruj parę kluczy (do podpisu i do jego weryfikacji): Podpis cyfrowy → PKI  Generowanie  Algorytm RSA – Długość modułu 2048 bitów  Wpisz swoje dane użytkownika (zapamiętaj PIN!)  Wygeneruj nową parę kluczy (postępuj zgodnie ze wskazówką pokazaną na ekranie);

 Pokaż pary kluczy

 Pokaż parametry publiczne

 Pokaż certyfikat

 Eksportuj plik PSE (PKCS #12)

Uwaga: plik z rozszerzenie **p12** zawiera obydwa klucze: publiczny i **prywatny**. Należy go dobrze chronić.

1. Pobierz ze strony <https://www.gpg4win.org/download.html> i zainstaluj aplikację Gpg4win [Gpg4win 4.0.3) – download the full version (including the Gpg4win compendium) of Gpg4win 2.3.0].
2. Uruchom program Kleopatra.
3. Tworzenie dokumentu CSR (*Certificate Signing Request*) z żądaniem certyfikatu X.509:

Plik  Nowa para kluczy…  Utworz pare osobistych kluczy X.509 i żądanie certyfikacji

Podaj szczegóły: Nazwisko (CN); adres e-mail; lokalizacja (L): (Poznan); jednostka organizacyjna (OU): WFiB; organizacja (O): WSB;kod kraju (C): PL  Dalej

W oknie pokazują się parametry certyfikatu  Pokaż wszystkie szczegóły  Utwórz – wpisz hasło chroniące klucz (zapamiętaj je!)

Zapisz plik z żądaniem certyfikatu wskazując katalog, w którym certyfikat będzie przechowywany (Zapisz żądanie certyfikatu do pliku…) – plik z rozszerzeniem **p10**.

Uwaga: kolejne kroki byłyby następujące (JEDNAK NIE BĘDZIEMY ICH WYKONYWAĆ!):

* Wyślij e-mail do www.cacert.org z żądaniem utworzenia certyfikatu (cacert.org jest niekomercyjnym CA).
* Gdy certyfikat zostanie przysłany można go importować go do aplikacji (np. Kleopatra, przeglądarka internetowa).

W celu emisji certyfikatu musisz mieć konto w CAcert uwierzytelnione przez innych członków CACert Web of Trust (informacje można znaleźć na stronach internetowych CAcert).

1. W sprawozdaniu należy zawrzeć:
2. Opis struktury certyfikatu X.509 (RFC 5280) (max 1 pkt).
3. Rezultaty wykonanych eksperymentów udokumentowane pobranymi wycinkami ekranów (max 5 pkt).
4. Wnioski (max 1 pkt).
5. Sprawozdanie należy umieścić na platformie Moodle w pliku o nazwie   
   09-nazwisko-imię.pdf   
   (wpisując w miejsce nazwisko-imię **swoje** nazwisko i imię).