Laboratorium Programowania Kart Elektronicznych

Certyfikaty

Marek Gosławski

Certyfikaty

- Przygotowanie do zajęć
  - aktywne eKonto
  - wygenerowany certyfikat
  - sprawna legitymacja studencka (lub inna karta)
- Potrzebne wiadomości
  - mechanizm podpisu elektronicznego (X.509)
  - umiejętność konfigurowania klienta poczty, wysyłania poczty elektronicznej
  - umiejętność korzystania z AdobeReader, OpenOffice Writer, Microsoft Word

„Słowniczek”

- **ustawy i rozporządzenia**
  - od 2001 r. do 2016 r. „o podpisie elektronicznym”
  - od 2014 r. Rozporządzenia Parlamentu Europejskiego i Rady (UE) w sprawie identyfikacji elektronicznej i usług zaufania (eIDAS)
  - od 2016 r. „o usługach zaufania oraz identyfikacji elektronicznej”

„Słowniczek”

- **podpis elektroniczny**
  - dane w postaci elektronicznej (…) służące do identyfikacji osoby składającej podpis *(do 2016)*
  - (…) które użyte są przez podpisującego jako podpis
- **zaawansowany podpis elektroniczny**
  - oznacza podpis elektroniczny, który spełnia wymogi określone w art. 26 *(eIDAS)*
    - *unikalne przyporządkowanie, możliwość ustalenia tożsamości, użyte dane znajdujące się pod wyłączną kontrolą, powiązany z danymi podpisywanymi sposób umożliwiający rozpoznanie zmiany*

„Słowniczek”

- **certyfikat**
  - elektroniczne zaświadczenie … dane … są przyporządkowane do osoby składającej podpis i które umożliwiają identyfikację tej osoby *(do 2016)*
- **certyfikat podpisu elektronicznego**
  - poświadczenie elektroniczne, które przyporządkowuje dane … do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby

„Słowniczek”

- **Middleware**
  - oprogramowanie umożliwiające współpracę systemu operacyjnego komputera z kartą
- **PKI** *(Public Key Infrastructure)*
  - … świadczenia usług …
    - uwierzytelniania,
    - szyfrowania,
    - integralności
    - niezaprzeczalności

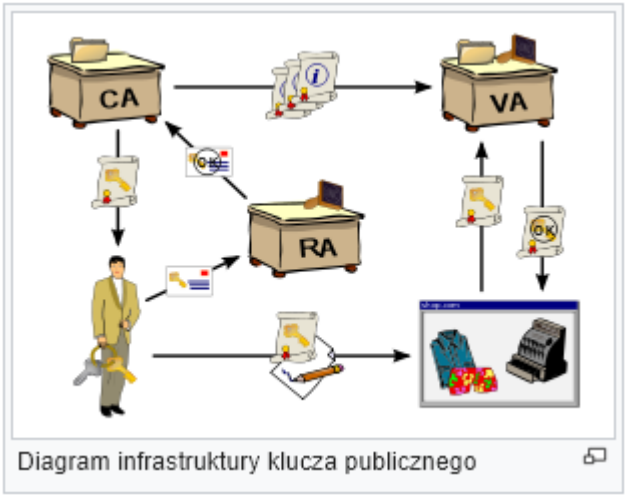
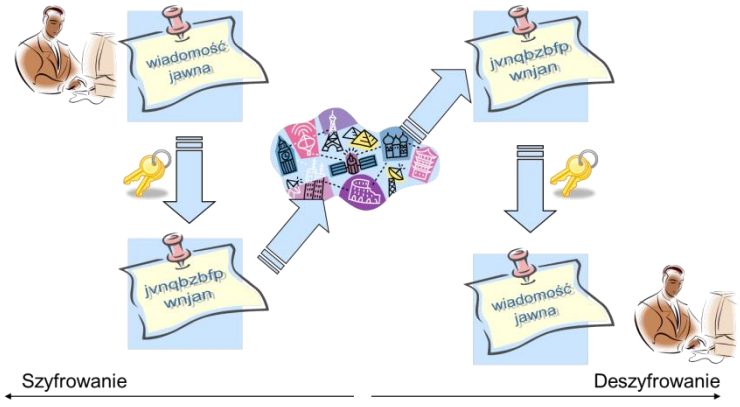


Diagram infrastruktury klucza publicznego

By Chris 論 - [1] and OpenCliparts.org, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=2501151

„Słowniczek”

- **Kryptografia symetryczna**
  - w algorytmach symetrycznych klucz służy do szyfrowania i deszyfrowania wiadomości

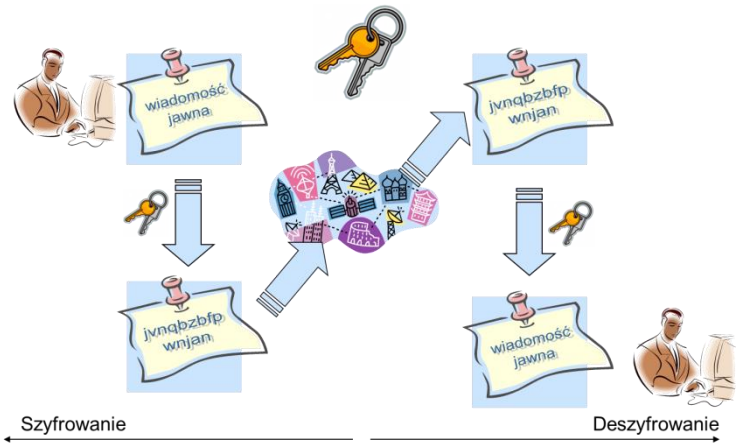


„Słowniczek”

- **Kryptografia asymetryczna**
  - w algorytmach asymetrycznych wyróżniamy **klucz publiczny** oraz **prywatny**:
    - prywatny – powinien znać tylko właściciel
    - publiczny – może być jawny
  - klucza powiązane zależnością matematyczną *(Diffie W., Hellman M., 1976)*
  - znajomość jednego nie pozwala na obliczenie drugiego, można upublicznić jeden z kluczy bez obniżenia poziomu bezpieczeństwa

„Słowniczek”

- **Kryptografia asymetryczna c.d.**
  - najważniejsze funkcje kryptografii asymetrycznej:
    - szyfrowanie – klucz publiczny służy do szyfrowania, a prywatny do deszyfrowania
    - podpisy cyfrowe – klucz prywatny służy do generowania podpisów, klucz publiczny do ich weryfikacji



„Słowniczek”

- **ELS**
  - Elektroniczna Legitymacja Studencka
- **ELD**
  - Elektroniczna Legitymacja Doktorancka

Certyfikaty

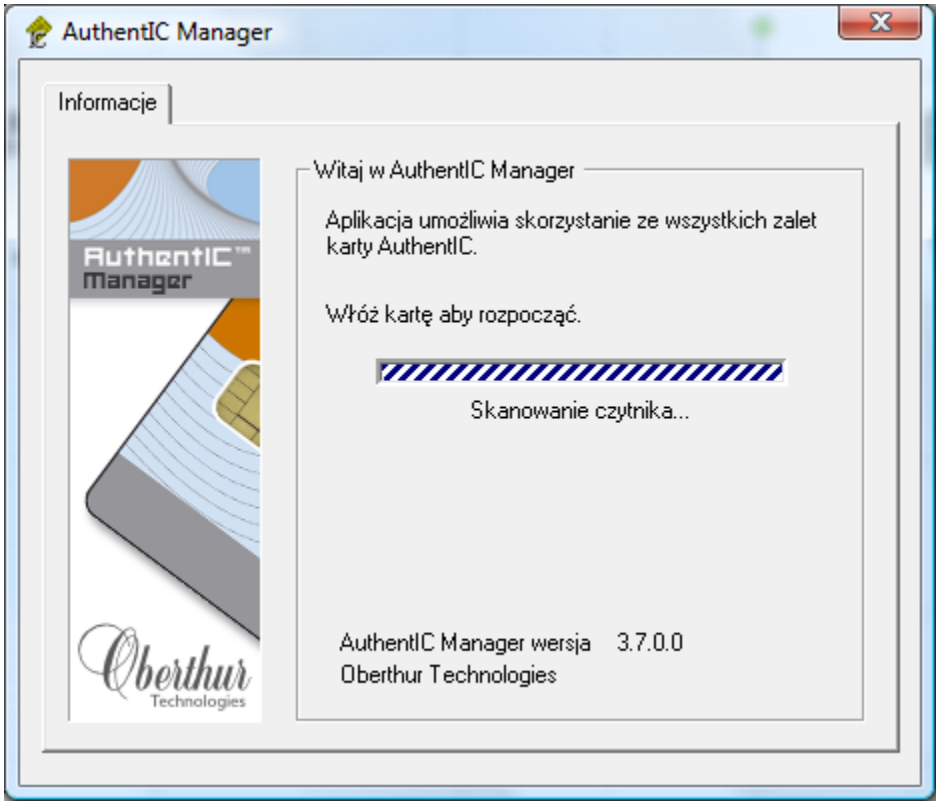
- Zadania
  - podpisanie wiadomości elektronicznej
  - zaszyfrowanie wiadomości elektronicznej
  - podpisanie dokumentu .pdf, .odt lub .doc(x)
  - weryfikacja podpisu kwalifikowanego
- Przesłanie na adres:
  - marek.goslawski@put.poznan.pl

Zadanie 1: podpisanie wiadomości elektronicznej
Zadanie 2: zaszyfrowanie wiadomości elektronicznej
Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x)
Zadanie 4: weryfikacja podpisu kwalifikowanego

wysłać na adres:
marek.goslawski@put.poznan.pl

Certyfikaty

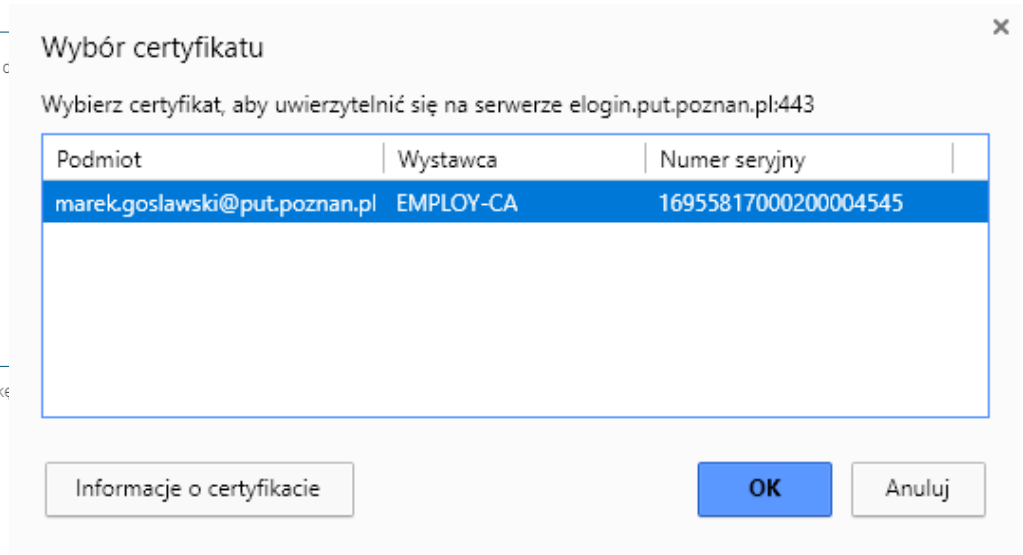
- Aktywacja funkcjonalności PKI na ELS
  - oprogramowanie AuthentIC WebPack lub ClassicClient
    - eProgramy
    - middleware
  - znajomość PUK karty
  - import certyfikatu
    - eLogin



Zadanie 1: podpisanie wiadomości elektronicznej
Zadanie 2: zaszyfrowanie wiadomości elektronicznej
Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x)
Zadanie 4: weryfikacja podpisu kwalifikowanego

Certyfikaty

- Logowanie certyfikatem na stronie eLogin
  - certyfikat musi być umieszczony w zasobniku systemu operacyjnego lub przeglądarki
  - klucz prywatny może być na karcie



Certyfikaty

- Bezpłatne certyfikaty S/MIME
  - do podpisywania poczty
  - wystawcy certyfikatów, przykłady *(09.2018)*
    - Actalis
    - Instant SSL (Comodo?)
    - Comodo
      - https://www.comodo.com/home/email-security/free-email-certificate.php

Certyfikaty

- Konfiguracja klienta poczty (Thunderbird)
  - konfiguracja konta imie.nazwisko@student.put.poznan.pl
    - dane konfiguracyjne: ePoczta

Zadanie 1: podpisanie wiadomości elektronicznej
Zadanie 2: zaszyfrowanie wiadomości elektronicznej
Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x)
Zadanie 4: weryfikacja podpisu kwalifikowanego

wysłać na adres:
marek.goslawski@put.poznan.pl

Certyfikaty

- Konfiguracja klienta poczty (Thunderbird)
  - konfiguracja konta do współpracy z kartą
    - ustawienia konta → zabezpieczenia → urządzenia zabezpieczeń → „wczytaj” *(wersja 32bit i 64bit!)*
      - C:\Program Files (x86)\Oberthur Technologies\AuthentIC Webpack\DLLs\OCSCryptoki.dll
      - C:\Program Files (x86)\Gemalto\Classic Client\BIN\gck2015x.dll
  - konfiguracja konta do podpisania wiadomości
    - wybór certyfikatu, wskazanie certyfikatu na karcie

Zadanie 1: podpisanie wiadomości elektronicznej
Zadanie 2: zaszyfrowanie wiadomości elektronicznej
Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x)
Zadanie 4: weryfikacja podpisu kwalifikowanego

wysłać na adres:
marek.goslawski@put.poznan.pl

Certyfikaty

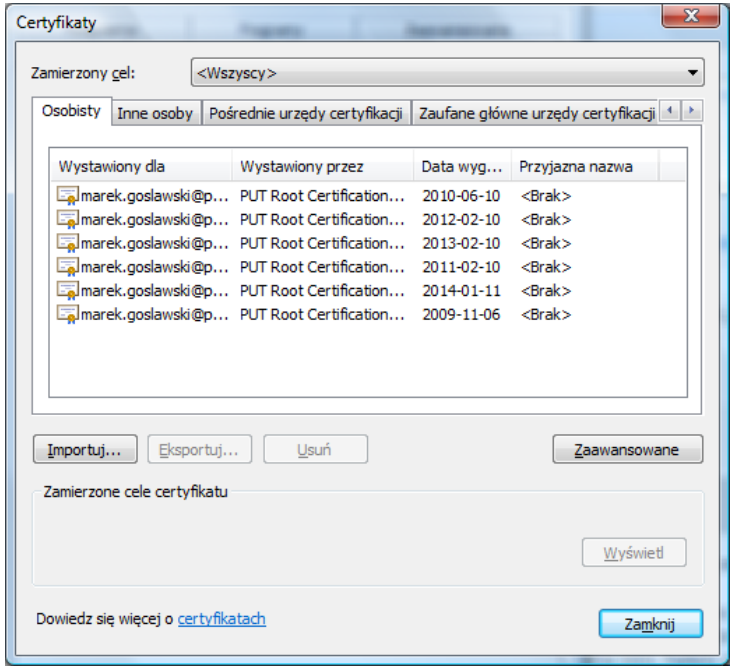
- Konfiguracja klienta poczty (Thunderbird)
  - konfigurowanie konta do szyfrowania wiadomości
    - https://elogin.put.poznan.pl/
    - manager certyfikatów
      - „urzędy certyfikacyjne” → dodanie certyfikatu ADENA/EMPLOY → „zaufaj … wiadomości”!
      - „twoje certyfikaty”
      - „inne osoby” → dodanie certyfikatu marek.goslawski@put.poznan.pl →„zaufaj …”

Zadanie 1: podpisanie wiadomości elektronicznej
Zadanie 2: zaszyfrowanie wiadomości elektronicznej
Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x)
Zadanie 4: weryfikacja podpisu kwalifikowanego

wysłać na adres:
marek.goslawski@put.poznan.pl

Certyfikaty

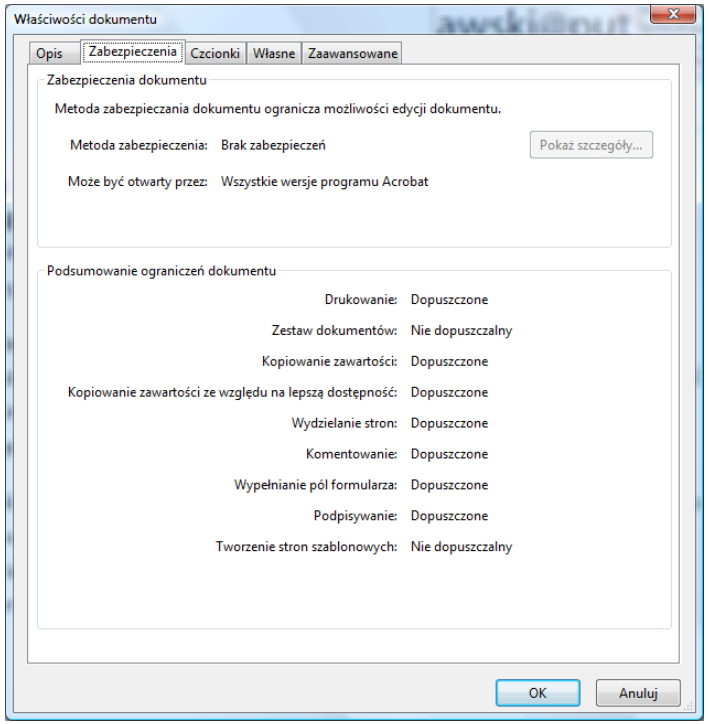
- Certyfikat w zasobniku Windows
  - mmc, „dodaj przystawkę”, „certyfikaty”
  - IE, „Narzędzia”, „Opcje internetowe”, „Zawartość”, „Certyfikaty”



Zadanie 1: podpisanie wiadomości elektronicznej
Zadanie 2: zaszyfrowanie wiadomości elektronicznej
Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x)
Zadanie 4: weryfikacja podpisu kwalifikowanego

Certyfikaty

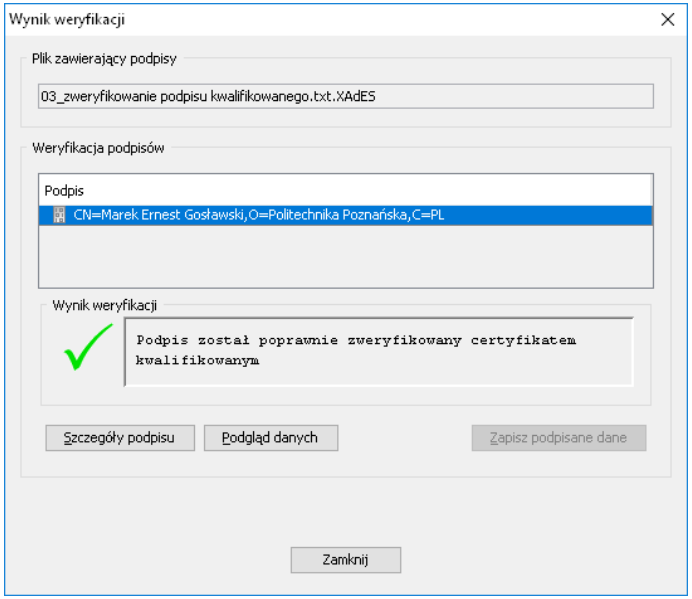
- Podpisanie dokumentów
  - 01. podpisywanie dokumentu AdobeReader (0/1/2).pdf
  - 01. podpisywanie dokumentu OpenOffice Writer.odt
  - 01. podpisywanie dokumentu MsWord.docx



Zadanie 1: podpisanie wiadomości elektronicznej
Zadanie 2: zaszyfrowanie wiadomości elektronicznej
Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x)
Zadanie 4: weryfikacja podpisu kwalifikowanego

Certyfikaty

- Weryfikacja podpisu kwalifikowanego
  - 03_zweryfikowanie podpisu kwalifikowanego.txt.XAdES



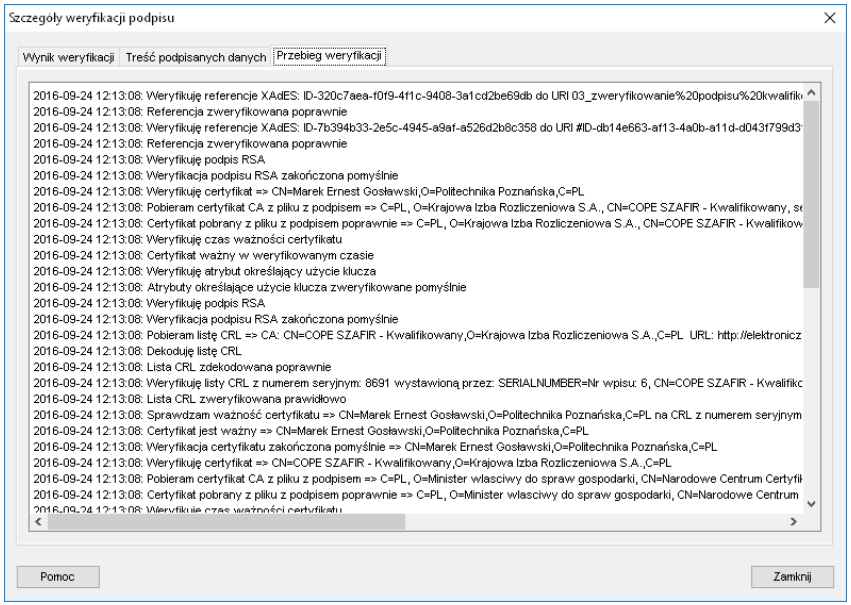
Zadanie 1: podpisanie wiadomości elektronicznej
Zadanie 2: zaszyfrowanie wiadomości elektronicznej
Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x)
Zadanie 4: weryfikacja podpisu kwalifikowanego

wysłać na adres:
marek.goslawski@put.poznan.pl

Certyfikaty

- Weryfikacja podpisu kwalifikowanego
  - jak?
  - podać kroki weryfikacji

1. Weryfikacja integralności dokumentu
2. Weryfikacja certyfikatu
   CN=Marek Ernest Gosławski,O=Politechnika Poznańska,C=PL
3. …



Zadanie 1: podpisanie wiadomości elektronicznej
Zadanie 2: zaszyfrowanie wiadomości elektronicznej
Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x)
Zadanie 4: weryfikacja podpisu kwalifikowanego

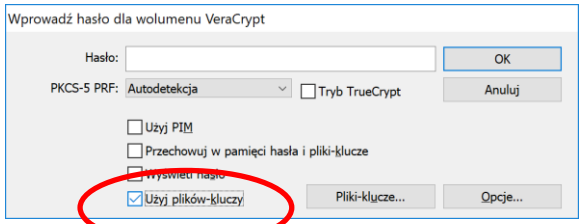
wysłać na adres:
marek.goslawski@put.poznan.pl

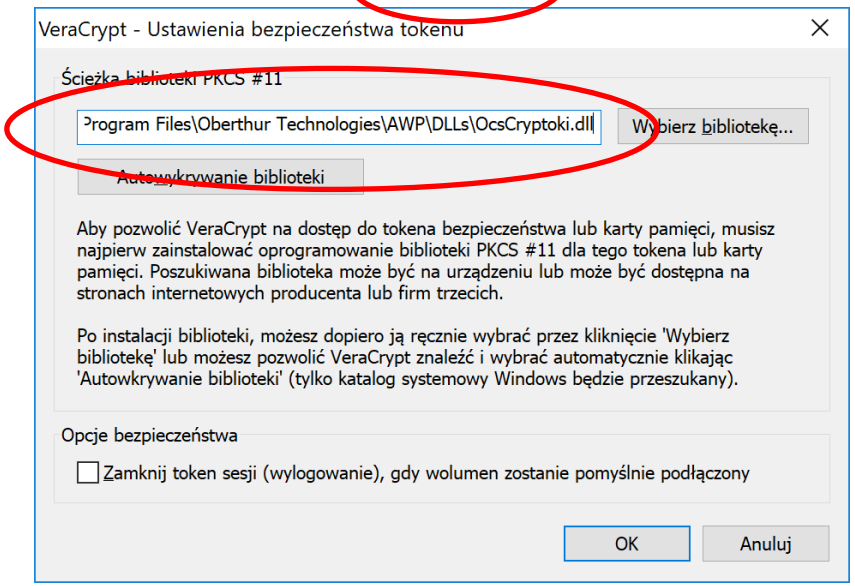
Certyfikaty

- ePUAP, PZ
  - https://obywatel.gov.pl/

Certyfikaty

- Konfigurowanie oprogramowania VeraCrypt
  - Ustawienia → Tokeny bezpieczeństwa
  - wskazanie biblioteki PKCS#11
  - „użyj plików kluczowych”
  - „dodaj token/bilet”





Zadanie 1: podpisanie wiadomości elektronicznej
Zadanie 2: zaszyfrowanie wiadomości elektronicznej
Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x)
Zadanie 4: weryfikacja podpisu kwalifikowanego

Certyfikaty

- **Nie zapomnij usunąć:**
  - **konta z klienta poczty (Thunderbird'a)!**
  - **certyfikatu z zasobników!**

- marek.goslawski@put.poznan.pl
- +48 61 665 3680
- +48 694 949 750
- pl. Marii Skłodowskiej-Curie 5 (Wilda)
  Budynek B1 (Rektorat), pok. 405

- http://mcp.poznan.pl/