Dostęp do strony www za pomocą certyfikatu znajdującego się na karcie (PKCS#11)

Sebastian Lewandowski

Agenda

1. Wymagania funkcjonalne
2. Środowisko
3. Zasoby i konfiguracja
4. Konfiguracja serwera - localhost
5. Konfiguracja serwera - VirtualHost
6. Architektura
7. Inne dostępne rozwiązania
8. Wymagania funkcjonalne - użycie

1. Wymagania funkcjonalne

- Dostęp do strony www za pomocą certyfikatu (put.poznna.pl) na PKCS(#11)
- Dostęp do strony www możliwy tylko dla użytkowników posiadających czytnik kart
- Odrzucenie próby dostępu do strony www , w przypadku braku karty w czytniku
- Odrzucenie próby dostępy do strony www, w przypadku braku certyfikatu na karcie
- Zapewnienie bezpieczeństwa poprzez uwierzytelnianie
- Zasoby www dostępne dla konkretnego użytkownika, posiadającego kartę (#PKCS11 oraz certyfikat)

2. Środowisko

- Serwer Apache/Ngnix/Tomcat
- Windows/Linux
- Localhost/virtual host/
- Browser : MozillaFirefox/Chrome/IE
- CryptoTech

3. Zasoby i konfiguracja

- Certyfikat – Sebastian.lewandowski@put.poznan.pl
  - Generowanie klucza prywatnego
- Konwertowanie pkcs#12 zawierającego klucz prywatny i certyfikat
- Root certificate – PUT POZNAN
- Konwertowanie (DER to PEM)
- Generowanie csr bazując na dotychczasowym certyfikacie i kluczu prywatnym
- Otwarcie połączenia ssl
- Konfigurowanie Apache (VirtualHost xxx:443)

4. Konfiguracja - localhost

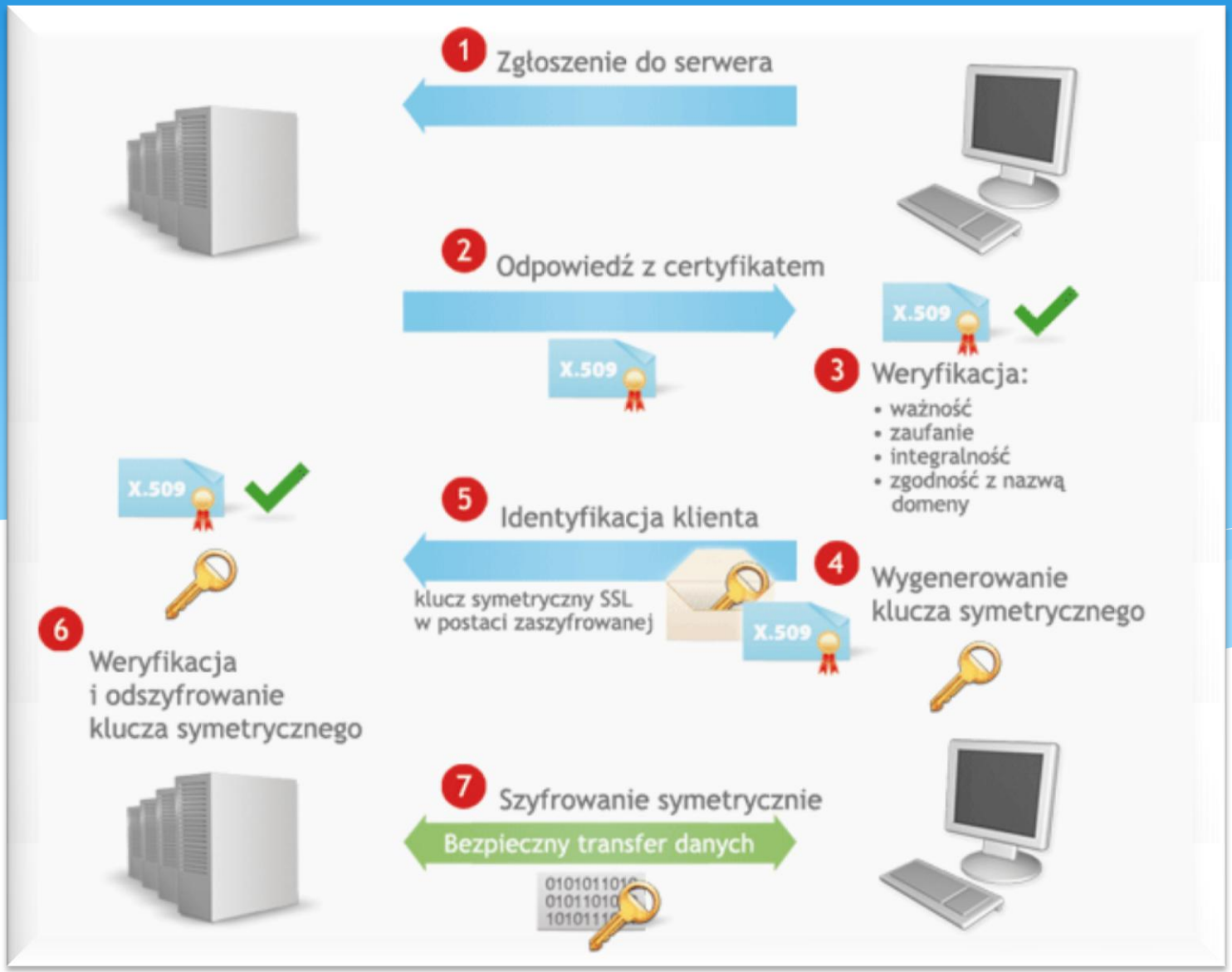
- Instalacje Apache na dysku
- Wykonanie poleceń z linii komend cmd (Windows):
  - openSSL connection
    - openssl pkcs12 –in [certyfikat.p12] –nodes –out private.key –nocerts
    - openssl x509 –in [katalog z plikiem root.cer] –out put.pem –outform PEM
    - openssl x509 –in [katalog z plikiem root.cer] –out put.der –outform DER
    - Restart Apache
  - konfiguracja Apache
  - Konfigurowanie przeglądarki (MozillaFirefox)
    - opcje -> certyfikaty -> urządzenia zabezpieczające
    - Wczytaj -> (ścieżka bibliotek programu np. AuthenticIC)

OpenSSL

4. Konfiguracja serwera - VirtualHost

- Dostęp do panelu administratora na serwerze
- Wgranie plików:
  - Root put poznan certyfikat
  - Sebastian.lewandowski@put .poznan.pl (p12)
  - Klucz prywatny

5. Architektura



5. Inne dostępne rozwiązania

- CryptoTech
- PKCS#11 moduł – MozillaFirefox

6. Wymagania funkcjonalne - użycie

Podziękuję za uwagę po teście