Kod szkolenia: **J/KRYPT**

Tytuł szkolenia: **Kryptografia na platformie Java w praktyce**

Dni: 3

Opis:

**Adresaci szkolenia**

Szkolenie adresowane jest do programistów tworzących aplikacje w środowisku Java.

**Cel szkolenia**

Celem szkolenia jest poznanie i praktyczne wykorzystanie różnorodnych technik zabezpieczeń i algorytmów kryptograficznych w języku Java. Uczestnicy poznają i użyją w praktyce mechanizmów służących do zapewnienia poufności, integralności i uwierzytelnienia oraz poznają cel stosowania algorytmów takich jak kody uwierzytelniające wiadomość, szyfrowanie z hasłem czy algorytmy podpisu cyfrowego. Poprzez przykłady realizowane w formie krótkich zadań programistycznych uczestnicy nabędą umiejętności prawidłowego wykorzystania omawianych mechanizmów na platformie Java.

**Mocne strony szkolenia**

Podczas warsztatów uczestnicy:

- skonfigurują i użyją wbudowanych mechanizmów Java związanych z bezpieczeństwem,
- użyją wybranych algorytmów kryptograficznych w celu zapewnienia usług integralności, uwierzytelnienia, niezaprzeczalności oraz poufności,
- zaimplementują protokół wzajemnego uwierzytelnienia pomiędzy kartą elektroniczną i aplikacją,
- wykorzystają protokół SSL/TLS do zapewnienia bezpiecznej komunikacji pomiędzy aplikacjami w Java,
- użyją urządzenia kryptograficznego za pomocą biblioteki PKCS#11.

**Wymagania**

Od uczestników wymagana jest podstawowa wiedza z zakresu programowania w języku Java.

**Specjalne wymagania techniczne**

Uczestnicy w trakcie zajęć korzystają z komputera z systemem Windows lub Linux. Niezbędne jest posiadanie co najmniej jednego czytnika kart elektronicznych zgodnego z PC/SC.

**Parametry szkolenia**

3 * 8 godzin (3 * 7 godzin netto) wykładów i warsztatów.

Program szkolenia:

1. Mechanizmy zabezpieczeń na platformie Java
    - zabezpieczenia na poziomie języka Java
    - polityki bezpieczeństwa
    - usługi uwierzytelniania i autoryzacji (*Java Authentication and Authorization Service*, JAAS)
    - *Java Cryptography Architecture* (JCA) i *Java Cryptographic Extension* (JCE)
    - konfiguracja dostawców usług kryptograficznych
    - biblioteka Bouncy Castle

2. Wprowadzenie do kryptografii
    - podstawowe usługi ochrony informacji: integralność, uwierzytelnienie, niezaprzeczalność i poufność
    - podstawowe zasady stosowane w kryptografii
    - bezpieczeństwo obliczeniowe i siła klucza
    - standaryzacja i zalecenia (RFC, ISO/IEC, CEN/CENELEC, ETSI, PKCS, FIPS, ANSI, ITSEC/Common Criteria)
    - notacja ASN.1, kodowanie DER i PEM

3. Przegląd algorytmów kryptograficznych na platformie Java
    - algorytmy symetryczne i asymetryczne
    - szyfry blokowe i ich parametry
    - AES, DES, 3DES i inne szyfry blokowe
    - podstawowe tryby pracy szyfrów blokowych (ECB, CBC, CTR)
    - szyfrowanie z hasłem (ang. *password based encryption*, PBE)
    - funkcje skrótu i ich zastosowania
    - MD5, rodzina SHA, algorytm Keccak
    - usługa uwierzytelnienia i identyfikacji
    - kody uwierzytelniające wiadomość: HMAC
    - bezpieczne kryptograficznie generatory ciągów pseudolosowych

- uwierzytelnione szyfrowanie (ang. *authenticated encryption*, AE)
- uwierzytelnione szyfrowanie z danymi dodatkowymi (ang. *authenticated encryption with additional data*, AEAD)
- tryby AE i AEAD: CCM, GCM
- algorytm Diffiego-Hellmana-Merkla (DH)
- algorytm RSA
- podpis cyfrowy i problem autentyczności klucza
- algorytm podpisu cyfrowego DSA
- algorytmy oparte o krzywe eliptyczne i ich parametry: ECDH i ECDSA
- szyfrowanie za pomocą algorytmów asymetrycznych
- podpis i szyfrowanie obiektów w Java

4. Bezpieczne przechowywanie kluczy

- repozytoria kluczy: JKS, JCEKS, PKCS#12, BC i BCFKS
- sprzętowe moduły bezpieczeństwa (ang. *hardware security module*, HSM)
- dostęp do urządzeń kryptograficznych: interfejs PKCS#11

5. Zastosowania kryptografii

- aktualne zalecenia dotyczące mechanizmów kryptograficznych (wykorzystywane algorytmy, długości kluczy i inne parametry)
- protokół zobowiązania bitowego
- protokół wyzwanie-odpowiedź
- znaczenie zaufania, zaufana trzecia strona (ang. *trusted third party*, TTP)
- infrastruktura klucza publicznego (ang. *public key infrastructure*, PKI)
- generowanie kluczy oraz zgłoszenia certyfikacyjnego
- certyfikaty X.509, rola pól i rozszerzeń certyfikatów, ścieżka certyfikacyjna
- lista certyfikatów unieważnionych (ang. *certificate revocation list*, CRL)
- protokół weryfikacji statusu certyfikatu (ang. *online certificate status protocol*, OCSP)
- działanie i parametry protokołu SSL/TLS
- *Java Secure Socket Extension* (JSSE)
- jednostronne i obustronne uwierzytelnienie w protokole SSL/TLS
- bezpieczna poczta elektroniczna S/MIME
- aplikacje dla kart kryptograficznych Java Card