Możliwość dofinansowania

Kryptografia na platformie Java w praktyce

Numer usługi 2025/07/20/10671/2889984

2 550,00 PLN brutto
2 550,00 PLN netto
106,25 PLN brutto/h
106,25 PLN netto/h

Sages Spółka z ograniczoną odpowiedzialnością

4,4 / 5

289 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
24 h
29.09.2025 do 01.10.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Programowanie
Grupa docelowa usługi	Szkolenie adresowane jest do programistów Java
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	22-09-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	24
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Poznanie i praktyczne wykorzystanie różnorodnych technik zabezpieczeń i algorytmów kryptograficznych w języku Java
Praktyczne użycie mechanizmów służących do zapewnienia poufności, integralności i uwierzytelnienia
Poznanie celu stosowania algorytmów - kody uwierzytelniające wiadomość, szyfrowanie z hasłem czy algorytmy podpisu cyfrowego
Zdobycie umiejętności prawidłowego wykorzystania mechanizmów na platformie Java, poprzez przykłady realizowane w formie krótkich zadań programistycznych

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik stosuje techniki zabezpieczeń i algorytmów kryptograficznych w języku Java, używa mechanizmów służących do zapewnienia poufności, integralności i uwierzytelnienia, stosuje algorytmy takie jak kody uwierzytelniające wiadomość, szyfrowanie z hasłem czy algorytmy podpisu cyfrowego, wykorzystuje mechanizmy na platformie Java.	Uczestnik stworzył realny projekt, który można wygodnie udostępnić, skomentować i zaprezentować.	Obserwacja w warunkach rzeczywistych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Mechanizmy zabezpieczeń na platformie Java

- Zabezpieczenia na poziomie języka Java
- Polityki bezpieczeństwa
- Usługi uwierzytelniania i autoryzacji (Java Authentication and Authorization Service, JAAS)
- Java Generic Security Services API (GSS-API)
- Java Cryptography Architecture (JCA) i Java Cryptographic Extension (JCE)
- Konfiguracja dostawców usług kryptograficznych
- Biblioteka Bouncy Castle

Wprowadzenie do kryptografii

- Podstawowe usługi ochrony informacji

- Integralność, uwierzytelnienie, niezaprzeczalność i poufność
- Podstawowe zasady stosowane w kryptografii
- Bezpieczeństwo obliczeniowe i siła klucza
- Podstawy notacji ASN.1
- Kodowanie DER (Distinguished Encoding Rules) i PEM (Privacy-Enhanced Mail)

Przegląd algorytmów kryptograficznych

- Algorytmy symetryczne i asymetryczne
- Szyfry blokowe i strumieniowe
- AES, ChaCha20, 3DES i inne szyfry symetryczne
- Podstawowe tryby pracy szyfrów blokowych: ECB, CBC, CTR
- Szyfrowanie z hasłem (password based encryption, PBE)
- Funkcje skrótu i ich zastosowania
- Rodzina SHA, SHA3 i algorytm Keccak
- Usługa uwierzytelnienia i identyfikacji
- Kody uwierzytelniające wiadomość: HMAC, KMAC i CMAC
- Funkcje wyprowadzania klucza (key derivation function, KDF)
- Bezpieczne kryptograficznie generatory ciągów pseudolosowych
- Tryby uwierzytelnionego szyfrowania (authenticated encryption, AE)
- Tryby uwierzytelnionego szyfrowania z danymi dodatkowymi (authenticated encryption with associated data, AEAD)
- Tryb CCM i GCM
- Algorytm Diffiego-Hellmana-Merkla (DH)
- Algorytm RSA
- Podpis cyfrowy i problem autentyczności klucza
- Krzywe eliptyczne w kryptografii: krzywe NIST, SECG i Brainpool, Curve25519, Curve448
- Algorytmy oparte o krzywe eliptyczne: ECDH, X25519, X448, ECDSA, EdDSA, Ed25519, Ed448
- Szyfrowanie za pomocą algorytmów asymetrycznych
- Podpis i szyfrowanie obiektów w Java
- Zalecenia dotyczące mechanizmów kryptograficznych (wykorzystywane algorytmy, długości kluczy i inne parametry)

Bezpieczne przechowywanie kluczy i haseł

- Repozytoria kluczy: PKCS #12, JKS, JCEKS, BC i BCFKS
- Karty inteligentne (smart cards)
- Elementy zabezpieczające (security elements, SE)
- Sprzętowe moduły zabezpieczeń (hardware security module, HSM)
- Interfejs PKCS #11
- Przechowywanie haseł: Argon2, bcrypt, PBKDF2

Zastosowania kryptografii

- Protokół zobowiązania bitowego
- Protokół wyzwanie-odpowiedź
- Java Simple Authentication and Security Layer (SASL)
- Znaczenie zaufania, zaufana trzecia strona (trusted third party, TTP)
- Infrastruktura klucza publicznego (public key infrastructure, PKI)
- Usługi PKI w kontekście usług ochrony informacji
- Generowanie kluczy oraz zgłoszenia certyfikacyjnego
- Certyfikaty X.509
- Łańcuch i ścieżka certyfikacji (certificate chain, certificate path)
- Repozytoria certyfikatów
- Pola certyfikatów i ich ustawienia
- Ograniczanie użycia klucza
- Lista certyfikatów unieważnionych (certificate revocation list, CRL)
- Protokół weryfikacji statusu certyfikatu (online certificate status protocol, OCSP)
- Bezpieczna poczta elektroniczna S/MIME
- Podpis cyfrowy, XML Digital Signature
- Działanie i parametry protokołu SSL/TLS
- Java Secure Socket Extension (JSSE)
- Jednostronne i obustronne uwierzytelnienie w protokole SSL/TLS
- Doskonałe utajnienie z wyprzedzeniem (perfect forward secrecy, PFS)

- Aplikacje dla kart kryptograficznych Java Card

Harmonogram

Liczba przedmiotów/zajęć: 3

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 3 Mechanizmy zabezpieczeń na platformie Java, Wprowadzenie do kryptografii	Piotr Nazimek	29-09-2025	09:00	17:00	08:00
2 z 3 Przegląd algorytmów kryptograficznych , Bezpieczne przechowywanie kluczy i haseł	Piotr Nazimek	30-09-2025	09:00	17:00	08:00
3 z 3 Zastosowania kryptografii	Piotr Nazimek	01-10-2025	09:00	17:00	08:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 550,00 PLN
Koszt przypadający na 1 uczestnika netto	2 550,00 PLN
Koszt osobogodziny brutto	106,25 PLN
Koszt osobogodziny netto	106,25 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Piotr Nazimek

Jestem inżynierem, obecnie prowadzę działalność gospodarczą. W 2012 roku obroniłem rozprawę doktorską z obszaru niezawodności systemów komputerowych na Politechnice Warszawskiej. Interesuję się szeroko pojętym bezpieczeństwem teleinformatycznym oraz inżynierią oprogramowania. Zawodowo pracuję od 2003 roku. Projektuję, implementuję i weryfikuję zabezpieczenia, głównie w projektach systemów transportowych i kontroli dostępu, które wykorzystują sprzętowe moduły bezpieczeństwa. Tworzyłem oprogramowanie dla bankomatów, terminali płatniczych i biletomatów, realizowałem projekty kart miejskich m. in. w Białymstoku, Tarnowie, Poznaniu i Krakowie. Jestem współtwórcą kasownika NV1. Jednym z niedawno realizowanych projektów była implementacja obsługi protokołu OSNMA służącego do uwierzytelnionego odbioru danych w europejskim systemie nawigacji satelitarnej Galileo. Prowadzę szkolenia komercyjne od 2012 roku. Brało w nich udział ponad 3000 osób. Specjalizuję się w szkoleniach z zakresu bezpieczeństwa takich jak: zastosowania algorytmów i protokołów kryptograficznych, infrastruktura klucza publicznego, wykorzystanie sprzętowych modułów bezpieczeństwa, bezpieczne programowane i bazy danych typu blockchain.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

materiały szkoleniowe - część teoretyczna szkolenia, slajdy - zostaną udostępnione uczestnikom na szkoleniu w formie pdf.

uczestnik otrzyma certyfikat uczestnictwa z opisem nabytych umiejętności

Warunki uczestnictwa

Od uczestników wymagane są podstawowe umiejętności z zakresu programowania w języku Java

Informacje dodatkowe

Szkolenie będzie prowadzone zdalnie, w czasie rzeczywistym, na żywo, z trenerem, możliwością zadawania pytań.

Szkolenie składa się w 30% z wykładu teoretycznego, w 70% z warsztatów i samodzielnej pracy programistycznej.

Podczas szkolenia uczestnicy mają dostęp do czatu z trenerem, współdzielą ekran podczas części warsztatowej, żeby zaprezentować postęp swojej pracy.

Walidacja będzie bazowała na ocenie efektów samodzielnej pracy uczestników, będzie sprawdzała nabytą wiedzę teoretyczną i umiejętność jej zastosowania w praktyce.

Warunki techniczne

szkolenie na platformie zoom, wymagane:

stabilne połączenie internetowe (zalecane min. 10Mbit/s download i 1Mbit/s upload)

przeglądarka internetowa Chrome

zainstalowana aplikacja Zoom App

dobrej jakości słuchawki oraz mikrofon (opcjonalnie) kamera internetowa

link do szkolenia zostanie przesłany uczestnikom przed szkoleniem i będzie aktywny do końca szkolenia.

Kontakt

Marta Sobczak

E-mail m.sobczak@sages.com.pl
Telefon (+48) 537 410 042