Możliwość dofinansowania

# Praktyczne aspekty stosowania kryptografii w systemach komputerowych

**Numer usługi** 2025/07/01/10671/2850401

4 305,00 PLN brutto
3 500,00 PLN netto
107,63 PLN brutto/h
87,50 PLN netto/h

Sages Spółka z ograniczoną odpowiedzialnością

4,4 / 5
288 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
40 h
20.10.2025 do 24.10.2025

# Informacje podstawowe

| | |
|---|---|
| **Kategoria** | Informatyka i telekomunikacja / Bezpieczeństwo IT |
| **Grupa docelowa usługi** | Szkolenie adresowane jest do programistów i architektów chcących poznać zagadnienia związane z prawidłowym wykorzystaniem mechanizmów kryptograficznych do budowy bezpiecznych systemów |
| **Minimalna liczba uczestników** | 4 |
| **Maksymalna liczba uczestników** | 8 |
| **Data zakończenia rekrutacji** | 10-10-2025 |
| **Forma prowadzenia usługi** | zdalna w czasie rzeczywistym |
| **Liczba godzin usługi** | 40 |
| **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 kryptograficznych, które używane są przy implementacji zabezpieczeń w systemach komputerowych
Poznanie prawidłowych zasad użycia między innymi algorytmów szyfrujących (symetrycznych i asymetrycznych), funkcji skrótu, kodów uwierzytelniających wiadomość, algorytmów podpisu cyfrowego oraz wybranych protokołów

kryptograficznych
Umiejętne unikanie typowych ataków na systemy wykorzystujące techniki kryptograficzne

### Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

| Efekty uczenia się | Kryteria weryfikacji | Metoda walidacji |
|---|---|---|
| Poznanie i praktyczne wykorzystanie różnorodnych technik kryptograficznych, które używane są przy implementacji zabezpieczeń w systemach komputerowych<br><br>Poznanie prawidłowych zasad użycia między innymi algorytmów szyfrujących (symetrycznych i asymetrycznych), funkcji skrótu, kodów uwierzytelniających wiadomość, algorytmów podpisu cyfrowego oraz wybranych protokołów kryptograficznych<br><br>Umiejętne unikanie typowych ataków na systemy wykorzystujące techniki kryptograficzne | Zrozumienie problemów związanych z zarządzaniem kluczami kryptograficznymi oraz przechowywaniem i przekazywaniem danych poufnych dzięki wielu praktycznym przykładom i warsztatom | Obserwacja w warunkach rzeczywistych |
| | Samodzielne zastosowanie poznanych mechanizmów do konfiguracji i uruchomienia centrum certyfikacji, zabezpieczonej poczty elektronicznej oraz komunikacji klient-serwer | Test teoretyczny |

# 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

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

Każdego dnia zajęcia w godz. 9:00-17:00, z przerwą na lunch około godz. 13:00

Wprowadzenie do ochrony informacji

Algorytmy symetryczne

Funkcje skrótu

Uwierzytelnienie i identyfikacja, kody uwierzytelniające wiadomość

Generatory liczb losowych

Szyfrowanie z uwierzytelnieniem

Algorytmy asymetryczne

Hasła

Protokoły kryptograficzne

Zarządzanie kluczami

Zastosowania kryptografii

Ataki na systemy wykorzystujące kryptografię

Walidacja

# Harmonogram

Liczba przedmiotów/zajęć: 5

| Przedmiot / temat zajęć | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|---|---|---|---|---|---|
| 1 z 5 **Wprowadzenie do ochrony informacji. Algorytmy symetryczne** | **Piotr Nazimek** | **20-10-2025** | **09:00** | **17:00** | **08:00** |
| 2 z 5 **Funkcje skrótu. Uwierzytelnienie i identyfikacja, kody uwierzytelniające wiadomość** | **Piotr Nazimek** | **21-10-2025** | **09:00** | **17:00** | **08:00** |
| 3 z 5 **Generatory liczb losowych Szyfrowanie z uwierzytelnieniem** | **Piotr Nazimek** | **22-10-2025** | **09:00** | **17:00** | **08:00** |

| Przedmiot / temat zajęć | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|---|---|---|---|---|---|
| 4 z 5 Algorytmy asymetryczne. Hasła. Protokoły kryptograficzne | Piotr Nazimek | 23-10-2025 | 09:00 | 17:00 | 08:00 |
| 5 z 5 Zarządzanie kluczami. Zastosowania kryptografii. Ataki na systemy wykorzystujące kryptografię | Piotr Nazimek | 24-10-2025 | 09:00 | 17:00 | 08:00 |

# Cennik

## Cennik

| Rodzaj ceny | Cena |
|---|---|
| **Koszt przypadający na 1 uczestnika brutto** | 4 305,00 PLN |
| **Koszt przypadający na 1 uczestnika netto** | 3 500,00 PLN |
| **Koszt osobogodziny brutto** | 107,63 PLN |
| **Koszt osobogodziny netto** | 87,50 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

część teoretyczna szkolenia, slajdy - zostanie przekazana uczestnikom na szkoleniu w formie pdf.

uczestnik otrzyma certyfikat uczestnictwa z opisem nabytych umiejętności

## Warunki uczestnictwa

Od uczestników wymagana jest znajomość obsługi komputera, pracy z wierszem poleceń oraz znajomość podstawowych zasad programowania i podstaw składni języków C i Java

## Informacje dodatkowe

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

# 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


### Agata Tuliszka-Kamińska

**E-mail** a.kaminska@sages.com.pl
**Telefon** (+48) 530 612 226