



Sages Spółka z
ograniczoną
odpowiedzialnością

★★★★☆ 4,4 / 5
310 ocen

Protokół SSL i TLS

Numer usługi 2026/02/21/10671/3352146

📍 zdalna w czasie rzeczywistym

📄 Usługa szkoleniowa

🕒 32 h

📅 13.04.2026 do 16.04.2026

4 735,50 PLN brutto

3 850,00 PLN netto

147,98 PLN brutto/h

120,31 PLN netto/h

196,00 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	• Programiści i administratorzy systemów z podstawową znajomością programowania oraz obsługi wiersza poleceń, chcący wdrażać i zarządzać bezpieczną komunikacją w aplikacjach • Specjaliści IT odpowiedzialni za bezpieczeństwo transmisji danych i integrację protokołów kryptograficznych w środowiskach produkcyjnych
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	10-04-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	32
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

Szkolenie przygotowuje do samodzielnej konfiguracji i wdrażania bezpiecznej komunikacji z użyciem protokołu SSL/TLS w aplikacjach i systemach informatycznych

Szkolenie uczy integrowania protokołu SSL/TLS z różnymi środowiskami programistycznymi oraz zarządzania

certifikatami i kluczami kryptograficznymi

Szkolenie pokazuje, jak analizować i stosować mechanizmy uwierzytelniania, zarówno oparte na certyfikatach PKI, jak i alternatywne metody

Szkolenie omawia zasady doboru i łączenia algorytmów

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik konfiguruje i uruchamia bezpieczne połączenia SSL/TLS w różnych środowiskach	Uczestnik integruje uwierzytelnianie oparte na certyfikatach i kartach inteligentnych	Obserwacja w warunkach rzeczywistych
Uczestnik analizuje i rozwiązuje problemy związane z bezpieczeństwem sesji SSL/TLS	Uczestnik ocenia i testuje konfiguracje pod kątem odporności na znane ataki	
Uczestnik projektuje i wdraża własny ośrodek certyfikacji oraz zarządza cyklem życia certyfikatów	Uczestnik wdraża rekomendowane praktyki migracji do kryptografii postkwantowej	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. Przerwa na lunch jest wliczona w czas usługi rozwojowej. Usługa prowadzona w godzinach zegarowych.

- 1. Wprowadzenie do ochrony informacji. Algorytmy i protokoły kryptograficzne - zajęcia teoretyczne, rozmowa na żywo, chat, współdzielenie ekranu
- 2. Mechanizm kapsułkowania kluczy (key encapsulation mechanism, KEM) - zajęcia teoretyczne, rozmowa na żywo, chat, współdzielenie ekranu
- 3. Przechowywanie i przekazywanie kluczy kryptograficznych - zajęcia praktyczne, ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu
- 4. Elementy i rola Infrastruktury Klucza Publicznego - zajęcia praktyczne, ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu
- 5. Działanie i konfiguracja protokołu SSL/TLS - zajęcia praktyczne, ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu
- 6. Integracja SSL/TLS w aplikacjach - zajęcia praktyczne, ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu
- 7. Protokół SSL/TLS w usłudze HTTPS - zajęcia praktyczne, ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu
- 8. Bezpieczeństwo protokołu SSL/TLS - zajęcia praktyczne, ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu
- 9. Walidacja - testy, ankiety - ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu

Harmonogram

Liczba przedmiotów/zajęć: 13

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 13 Wprowadzenie do ochrony informacji. Algorytmy i protokoły kryptograficzne - zajęcia teoretyczne, rozmowa na żywo, chat, współdzielenie ekranu	Piotr Nazimek	13-04-2026	09:00	13:00	04:00
2 z 13 Przerwa na lunch jest wliczona w czas usługi rozwojowej.	Piotr Nazimek	13-04-2026	13:00	13:15	00:15
3 z 13 Mechanizm kapsułkowania kluczy (key encapsulation mechanism, KEM) - zajęcia teoretyczne, rozmowa na żywo, chat, współdzielenie ekranu	Piotr Nazimek	13-04-2026	13:15	17:00	03:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 13 Przechowywanie i przekazywanie kluczy kryptograficznych - zajęcia praktyczne, ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Piotr Nazimek	14-04-2026	09:00	13:00	04:00
5 z 13 Przerwa na lunch jest wliczona w czas usługi rozwojowej.	Piotr Nazimek	14-04-2026	13:00	13:15	00:15
6 z 13 Elementy i rola Infrastruktury Klucza Publicznego - zajęcia praktyczne, ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Piotr Nazimek	14-04-2026	13:15	17:00	03:45
7 z 13 Działanie i konfiguracja protokołu SSL/TLS - zajęcia praktyczne, ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Piotr Nazimek	15-04-2026	09:00	13:00	04:00
8 z 13 Przerwa na lunch jest wliczona w czas usługi rozwojowej.	Piotr Nazimek	15-04-2026	13:00	13:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 13 Integracja SSL/TLS w aplikacjach - zajęcia praktyczne, ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Piotr Nazimek	15-04-2026	13:15	17:00	03:45
10 z 13 Protokół SSL/TLS w usłudze HTTPS - zajęcia praktyczne, ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Piotr Nazimek	16-04-2026	09:00	13:00	04:00
11 z 13 Przerwa na lunch jest wliczona w czas usługi rozwojowej.	Piotr Nazimek	16-04-2026	13:00	13:15	00:15
12 z 13 Bezpieczeństwo protokołu SSL/TLS - zajęcia praktyczne, ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Piotr Nazimek	16-04-2026	13:15	16:30	03:15
13 z 13 Walidacja - testy, ankiety - ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Piotr Nazimek	16-04-2026	16:30	17:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
-------------	------

Koszt przypadający na 1 uczestnika brutto	4 735,50 PLN
Koszt przypadający na 1 uczestnika netto	3 850,00 PLN
Koszt osobogodziny brutto	147,98 PLN
Koszt osobogodziny netto	120,31 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 programowanie 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 - prowadzone będą listy obecności, frekwencja minimum 80% wymagana do zaliczenia szkolenia

Warunki uczestnictwa

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

Informacje dodatkowe

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

Szkolenie składa się z wykładu teoretycznego oraz z warsztatów i samodzielnej pracy.

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



Agata Tuliszka-Kamińska

E-mail a.kaminska@sages.com.pl

Telefon (+48) 530 612 226