



Dagma sp. z o.o.

★★★★★ 4,5 / 5

454 oceny

PKI - Infrastruktura Klucza Publicznego w Windows Server

Numer usługi 2026/01/20/17164/3269604

- 📄 Usługa szkoleniowa
- 📄 zdalna w czasie rzeczywistym
- 🕒 28:00 h
- 📅 20.10.2026 do 23.10.2026

4 292,70 PLN brutto

3 490,00 PLN netto

153,31 PLN brutto/h

124,64 PLN netto/h

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

Szkolenie z zakresu Public Key Infrastructure, pozwoli na zapoznanie się z nowoczesnymi metodami ochrony informacji w oparciu o rolę AD CS w Windows Server.

Wymagania

- dobra znajomość zagadnień z zakresu administracji systemami komputerowymi,
- umiejętność instalacji oprogramowania, edycji plików konfiguracyjnych, obsługa konsoli,
- znajomość zagadnień sieciowych.

Minimalna liczba uczestników

5

Maksymalna liczba uczestników

10

Data zakończenia rekrutacji

12-10-2026

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

Liczba godzin usługi

28

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

Wiedza uzyskana po tym szkoleniu pozwoli na:

projektowanie, wdrożenie i utrzymanie infrastruktury klucza publicznego, rozbudowę funkcjonalności PKI, obsługę procesu zgłoszeń certyfikacyjnych, wystawianie i obsługę certyfikatów o różnym przeznaczeniu.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozumie koncepcje i architekturę infrastruktury klucza publicznego (PKI).	Uczestnik potrafi opisać, czym jest PKI, jakie elementy wchodzi w skład infrastruktury (CA, certyfikaty, szablony, polityki) oraz jakie są role usług certyfikacji w środowisku Windows Server.	Obserwacja w warunkach symulowanych
Uczestnik potrafi zaplanować i wdrożyć usługę Active Directory Certificate Services (AD CS).	Uczestnik umie zaplanować strukturę PKI dostosowaną do potrzeb organizacji oraz przeprowadzić instalację i konfigurację CA w środowisku Windows Server.	Obserwacja w warunkach symulowanych
Uczestnik potrafi zarządzać cyklem życia certyfikatów i szablonów.	Uczestnik umie tworzyć, edytować i wdrażać szablony certyfikatów, zarządzać wydawaniem, odnowieniem i odwoływaniem certyfikatów w środowisku Windows.	Obserwacja w warunkach symulowanych
Uczestnik zna zasady zabezpieczania i monitorowania infrastruktury PKI.	Uczestnik potrafi wskazać najlepsze praktyki bezpieczeństwa (np. offline root CA, zabezpieczenie kluczy prywatnych, CRL/OCSP, hardening) oraz monitorować stan CA i usługi PKI.	Obserwacja w warunkach symulowanych

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

1. Wprowadzenie do PKI.
2. Historia i przegląd metod kryptograficznych.
3. Certyfikaty elektroniczne.
4. Wdrożenia – planowanie, wdrażanie urzędów certyfikacji w oparciu o wykorzystanie symulatora Hardware Security Module (HSM).
5. Konfiguracja punktu dystrybucji listy odwołanych certyfikatów (CRL) oraz serwera weryfikacji statusu certyfikatów (OCSP).
6. Zarządzanie szablonami certyfikatów.
7. Korzystanie z certyfikatów komputera na przykładzie protokołu SSL/TLS.
8. Zastosowanie certyfikatów użytkownika z wykorzystaniem (wirtualnych) kart inteligentnych.
9. Konfiguracja roli agenta rejestracji certyfikatów.
10. Wdrożenie roli agenta odzyskiwania kluczy.
11. Wdrożenie EFS w oparciu o urząd certyfikacji z uwzględnieniem roli agenta odzyskiwania danych.
12. Wskazówki dotyczące konfiguracji usługi rejestracji certyfikatów dla urzędów sieciowych i mobilnych (NDES).
13. Zarządzania, utrzymanie i monitorowanie urzędu certyfikacji.
14. Opracowanie scenariuszy wysokiej odporności na awarie dla urzędów certyfikacji.
15. Przegląd dostępnych rozwiązań w zakresie zarządzania urządzeniami certyfikacji jak i samymi certyfikatami.

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 292,70 PLN
Koszt przypadający na 1 uczestnika netto	3 490,00 PLN
Koszt osobogodziny brutto	153,31 PLN
Koszt osobogodziny netto	124,64 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Adam Jakubiec

Trener IT w Dagma Szkolenia IT od 2015 roku, prowadzący szkolenia z dziedziny systemów informatycznych, Technologii Microsoft, cyberbezpieczeństwa, infrastruktura klucza publicznego (PKI).

Kierownik działu IT w międzynarodowym przedsiębiorstwie, wykładowca akademicki, trener technologii Microsoft oraz licznych autorskich i autoryzowanych kursów z zakresu bezpieczeństwa infrastruktury teleinformatycznej. Uzyskane certyfikacje: C)TIA: Certified Threat Intelligence Analyst; AZ-900 Microsoft Azure Fundamentals; C)PSH: Certified Powershell Hacker; C)PTE: Certified Penetration Testing Engineer; 70-744 Securing Windows Server 2016; 70-743 Upgrading Your Skills to MCSA: Windows Server 2016; 74-409 Server Virtualization with Windows Server Hyper-V and System Center; 70-698 Configuring Windows 10; Microsoft Certified Trainer, 70-640 Windows Server 2008 Active Directory, Configuration, Wykształcenie: wyższe, Edukacja informatyczno-techniczna, Aplikacje komputerowe (MCA).

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (prezentacja, do której dostęp zostanie udostępniony na adres e-mail uczestnika)

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową <https://szkolenia.dagma.eu/pl> w celu rezerwacji miejsca.

Informacje dodatkowe

- Jedna godzina lekcyjna to 45 minut
- W cenę szkolenia nie wchodzi koszt związany z dojazdem, wyżywieniem oraz noclegiem.
- Szkolenie nie zawiera egzaminu.
- Uczestnik otrzyma zaświadczenie DAGMA Szkolenia IT o ukończeniu szkolenia
- Uczestnik ma możliwość złożenia reklamacji po zrealizowanej usłudze, sporządzając ją w formie pisemnej (na wniosku reklamacyjnym) i odsyłając na adres szkolenia@dagma.pl. Reklamacja zostaje rozpatrzona do 30 dni od dnia otrzymania dokumentu przez DAGMA SZKOLENIA IT

Warunki techniczne

a) platforma/rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa:

- **ZOOM lub MS Teams**
- w przypadku kilku uczestników przebywających w jednym pomieszczeniu, istnieją dwie możliwości udziału w szkoleniu:

1) każda osoba bierze udział w szkoleniu osobno (korzystając z oddzielnych komputerów), wówczas należy wyciszyć dźwięki z otoczenia by uniknąć sprzężeń;

2) otrzymujecie jedno zaproszenie, wówczas kilka osób uczestniczy w szkoleniu za pośrednictwem jednego komputera

- Można łatwo udostępnić sobie ekran, oglądać pliki, bazę handlową, XLS itd.

b) minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji:

- Uczestnik potrzebuje komputer z przeglądarką Chrome lub Edge (NIE firefox), mikrofon, głośniki.

c) minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik:

- łącze internetowe o przepustowości minimum 10Mbit,

d) niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów:

- uczestnik na tydzień przed szkoleniem otrzyma maila organizacyjnego, ze szczegółową instrukcją pobrania darmowej platformy ZOOM.
- Z platformy MS Teams można korzystać za pośrednictwem przeglądarki, nie trzeba nic instalować.

e) okres ważności linku:

- link będzie aktywny od pierwszego dnia rozpoczęcia się szkolenia do ostatniego dnia trwania usługi

Szczegóły, związane z prowadzonymi przez nas szkoleniami online, znajdziesz na naszej stronie: <https://szkolenia.dagma.eu/pl/training-list>

Kontakt



Michalina Krzyszkowska

E-mail krzyszkowska.m@dagma.pl

Telefon (+48) 327 931 015