

Szkolenie: Microsoft  
Infrastruktura Klucza Publicznego (PKI) w Windows Server 2012, 2012 R2  
i 2016

FORMA SZKOLENIA	MATERIAŁY SZKOLENIOWE	CENA	CZAS TRWANIA
Stacjonarne	Cyfrowe	3200 PLN NETTO*	4 dni
Stacjonarne	Tablet CTAB	3600 PLN NETTO*	4 dni

\* (+VAT zgodnie z obowiązującą stawką w dniu wystawienia faktury)

## LOKALIZACJE

Kraków - ul. Tatarska 5, II piętro, godz. 9:00 - 16:00

Warszawa - ul. Bielska 17, godz. 9:00 - 16:00

## DOSTĘPNE TERMINY

2019-08-19 | 4 dni | Warszawa

2019-09-09 | 4 dni | Warszawa

2019-10-21 | 4 dni | Kraków

2019-11-25 | 4 dni | Warszawa

## Cel szkolenia:

Uczestnicy szkolenia **Infrastruktura Klucza Publicznego (PKI) w Windows Server 2012, 2012 R2 i 2016** zostaną zapoznani z nowoczesnymi metodami **ochrony informacji** w oparciu o rolę **AD CS w Windows Server**. Wiedza i umiejętności zdobyte podczas kursu IT pozwolą na **projektowanie, wdrożenie i utrzymanie infrastruktury klucza publicznego**.

Każdy z uczestników uruchomi własne **centrum certyfikacji**, które pozwoli poznać proces obsługi zgłoszeń certyfikacyjnych w celu wystawiania i obsługi certyfikatów o różnym przeznaczeniu: uwierzytelnienie w protokole SSL/TLS, podpis cyfrowy w odniesieniu do dokumentów, skryptów i oprogramowania, serwer weryfikacji statusu certyfikatów (OCSP), dwuskładnikowe uwierzytelnianie przy użyciu kart inteligentnych czy szyfrowania plików z wykorzystaniem EFS.

Szkolenie obejmuje swoim zakresem także możliwość rozszerzenia zakresu **infrastruktury klucza publicznego** w oparciu o możliwość nawiązania relacji zaufania z partnerskimi **urzędami certyfikacji**.

## Plan szkolenia:

- Wprowadzenie do PKI. Historia i przegląd metod kryptograficznych. Certyfikaty elektroniczne.
- Nowości w AD CA w Windows Server 2012, 2012 R2 i 2016.

- Strategie wdrożenia – planowanie, wdrażanie (w tym upgrade i migracja) urzędu certyfikacji; również w oparciu o wykorzystanie Hardware Security Module (HSM).
- Zarządzanie szablonami certyfikatów.
- Zarządzania, utrzymanie i monitorowanie urzędu certyfikacji.
- Opracowanie scenariuszy wysokiej odporności na awarie dla urzędów certyfikacji.
- Konfiguracja punktu dystrybucji listy odwołanych certyfikatów (CRL) i serwera weryfikacji statusu certyfikatów (OCSP).
- Metody dystrybucji certyfikatów elektronicznych w środowisku AD DS oraz dla użytkowników zewnętrznych. Omówienie funkcjonalności Roaming Credentials.
- Korzystanie z certyfikatów komputera na przykładzie protokołu SSL/TLS.
- Zabezpieczenie tunelu VPN z wykorzystaniem certyfikatu – uwierzytelnianie serwera i użytkownika, szyfrowanie danych.
- Zastosowanie certyfikatów użytkownika z wykorzystaniem kart inteligentnych. Konfiguracja roli agenta rejestracji certyfikatów.
- Wdrożenie roli agenta odzyskiwania kluczy.
- Wdrożenie EFS w oparciu o urząd certyfikacji z uwzględnieniem roli agenta odzyskiwania danych.
- Wskazówki dotyczące usługi rejestracji urządzeń sieciowych (NDES).
- Scenariusze relacji zaufania pomiędzy organizacjami partnerskimi na poziomie CA.
- Przegląd możliwości narzędzi wiersza poleceń – certreq.exe i certutil.exe oraz modułów PowerShell.

## Poziom trudności



## Certyfikaty:

Uczestnicy szkolenia **Infrastruktura Klucza Publicznego (PKI) w Windows Server 2012, 2012 R2 i 2016** otrzymują **certyfikat** wystawiony imiennie oraz na firmę, sygnowany przez **Microsoft**.

## Prowadzący:

Microsoft Certified Trainer.