

Kryptografia

Użytkowe aspekty zastosowania kart kryptograficznych IBM 4764 (CPH01) – 2 dni

Zakres tematyczny:

Karta IBM 4764 jest jedyną dostępną na rynku polskim kartą kryptograficzną certyfikowaną przez *National Institute of Standards and Technology* na poziomie FIPS 140-2 level 4. W trakcie szkolenia zostaną przedstawione potencjalne sposoby zastosowania kart kryptograficznych dostępnych w serwerach IBM. Zostaną zademonstrowane tryby wykorzystania kart, jako *akceleratorów* kryptograficznych oraz w pełni funkcjonalnych urządzeń typu *Hardware Security Module*. Praktyczne aspekty ich wykorzystania obejmują m.in. komunikację w protokole TLS, generowanie liczb losowych oraz kluczy RSA, jak również kompresję i szyfrowanie danych. Na życzenie klienta istnieje możliwość skoncentrowania się na implementacjach funkcji w jednym z wybranych systemów operacyjnych: AIX, i5/OS, z/OS lub Linux w oparciu o biblioteki Common Cryptographic Architecture i PKCS #11.

Przeznaczenie kursu:

Kurs jest przeznaczony dla administratorów systemów informatycznych, architektów oraz programistów aplikacji wykorzystujących funkcje kryptograficzne infrastruktury klucza publicznego lub algorytmy szyfrowania symetrycznego.

Oczekiwane umiejętności:

- administracja wybranym systemem operacyjnym (AIX, i5/OS, z/OS lub Linux) w stopniu podstawowym
- podstawowa umiejętność pisania skryptów lub programów języka sterującego (CL/JCL)

Cel:

Po ukończeniu kursu uczestnik powinien umieć:

- skonfigurować kartę kryptograficzną IBM 4764
- przygotować system operacyjny do współpracy z kartą kryptograficzną
- wykorzystać kartę kryptograficzną w wybranym scenariuszu i wybranym trybie
- kontrolować i monitorować pracę urządzenia kryptograficznego

Programowanie aplikacji z wykorzystaniem usług kryptograficznych kart IBM 4764 (CPH02) – 3 dni

Zakres tematyczny:

Karta IBM 4764 jest jedyną dostępną na rynku polskim kartą kryptograficzną certyfikowaną przez *National Institute of Standards and Technology* na poziomie FIPS 140-2 level 4. Szkolenie prowadzone w formie warsztatów obejmuje zagadnienia związane z praktycznym wykorzystaniem przez programistów funkcji kryptograficznych udostępnianych przez karty IBM 4764. W trakcie szkolenia zostaną przedstawione metody dostępu do usług kryptograficznych w oparciu o standardy PKCS #11, Common Cryptographic Architecture oraz Java Cryptographic Extension. W trakcie ćwiczeń uczestnicy poznają sposoby wykorzystania kart, zarówno jako *akceleratorów* kryptograficznych oraz urządzeń typu *Hardware Security Module*. Na życzenie klienta istnieje możliwość sprofilowania szkolenia i skoncentrowania się na implementacjach funkcji w jednym z wybranych systemów operacyjnych: AIX, i5/OS, z/OS lub Linux.

Przeznaczenie kursu:

Kurs jest przeznaczony dla administratorów systemów informatycznych, architektów oraz programistów aplikacji wykorzystujących funkcje kryptograficzne infrastruktury klucza publicznego lub algorytmy szyfrowania symetrycznego.

Oczekiwane umiejętności:

- znajomość architektury i scenariuszy wykorzystania kart IBM 4764 na poziomie kursu CPH01
- umiejętność pisania skryptów lub programów języka sterującego (CL/JCL)
- umiejętność programowania w języku C lub Java na poziomie średnio-zaawansowanym

Cel:

Po ukończeniu kursu uczestnik powinien umieć:

- wykorzystać kartę kryptograficzną w wybranym scenariuszu i wybranym trybie
- kontrolować i monitorować pracę urządzenia kryptograficznego
- przeprowadzać proste testy funkcjonalne i wydajnościowe