POLITECHNIKA CZĘSTOCHOWSKA
WYDZIAŁ INŻYNIERII MECHANICZNEJ I INFORMATYKI

Sprawozdanie
Tworzenie infrastruktury klucza prywatnego

Piotr Zyszczak i Damian Łukasik

Nr albumu: 113066/112993

Kierunek: Informatyka

Studia: stacjonarne

Poziom studiów: II

Częstochowa, 2015

Spis treści

1. Cel i zakres zajęć

Celem zajęć było stworzenie Infrastruktury Klucza Publicznego

2. Wstęp teoretyczny

Infrastruktura klucza publicznego (ang. Public Key Infrastructure (PKI)) – zbiór osób, polityk, procedur i systemów komputerowych niezbędnych do świadczenia usług uwierzytelniania, szyfrowania, integralności i niezaprzeczalności za pośrednictwem kryptografii klucza publicznego i prywatnego i certyfikatów elektronicznych. W szczególności jest to szeroko pojęty kryptosystem, w skład którego wchodzą urzędy certyfikacyjne (CA), urzędy rejestracyjne (RA), subskrybenci certyfikatów klucza publicznego (użytkownicy), oprogramowanie oraz sprzęt. Infrastruktura klucza publicznego tworzy hierarchiczną strukturę zaufania, której podstawowym dokumentem jest certyfikat klucza publicznego. Najpopularniejszym standardem certyfikatów PKI jest X.509 w wersji trzeciej. Do podstawowych funkcji PKI należą:

- Weryfikacja tożsamości subskrybentów
- Wymiana kluczy kryptograficznych
- Wystawianie certyfikatów
- Weryfikacja certyfikatów
- Podpisywanie przekazu
- Szyfrowanie przekazu
- Potwierdzanie tożsamości
- Znakowanie czasem

Dodatkowo, w pewnych konfiguracjach, możliwe jest:

- Odzyskiwanie kluczy prywatnych.

3. Przebieg

Najpierw dodajemy rolę serwer aplikacji do serwera. Następnie zaznaczamy obsługę serwera sieci web i role serwera sieci web (IIS). Sprawdzamy czy usługi działają odwołując się w przeglądarce do localhosta.

Kolejny krok to Główny Urząd Certyfikacji. Instaluje się w tym celu kolejną rolę Urząd certyfikacji w usłudze Active Directory.

Urząd zainstalowany został poprzez wybór poniższych opcji:

- tryb instalacji jako automatyczny,
- typ urzędu jako główny urząd certyfikacji,
- klucz prywatny jako nowy klucz prywatny,
- kryptografia bez zmian,
- nazwa urzędu certyfikacji - wpisujemy nazwę utworzonego kontrolera,
- okres ważności i ścieżka bez zmian

Pod adresem http://localhost/certsrv/ możemy sprawdzić poprawność działania aplikacji internetowej wchodzącej w skład zainstalowanej nowo roli serwera.

Pośredni Urząd Certyfikacji instaluję się podobnie jak Główny, z wyjątkiem:

- typ urzędu ustawiamy na podrzędny,
- nazwa urzędu np.: klient

4. Wnioski

Klucz publiczny stosuje się przede wszystkim z powodu bezpieczeństwa. Ponadto daje nam to uproszczoną administrację, gdzie organizacją może wystawić certyfikaty, tak, aby wyeliminować ciągłe stosowanie haseł. Ponadto istnieje możliwość bezpiecznej wymiany plików i danych w sieciach publicznych taki jak Internet.