

# Tendencje infrastruktury publicznego

# rozwojowe klucza

>

## **Wprowadzenie .....9**

### **1. Podstawy kryptografii .....11**

#### 1.1. Kryptografia symetryczna .....13

##### 1.1.1. Algorytm DES i jego modyfikacje .....16

##### 1.1.2. Algorytm IDEA .....18

##### 1.1.3. Algorytm Rijndael – AES .....20

##### 1.1.4. Algorytmy Ronalda Rivesta (RCx) .....22

#### 1.2. Kryptografia asymetryczna .....25

##### 1.2.1. Algorytm wymiany kluczy Diffiego-Hellmana .....27

##### 1.2.2. System RSA .....29

##### 1.2.3. Algorytm ElGamala .....31

#### 1.3. Funkcja skrótu i HMAC .....33

##### 1.3.1. Funkcja VMPC – polski akcent w światowej kryptografii .....35

#### 1.4. Podpis cyfrowy (elektroniczny) .....36

##### 1.4.1. Tworzenie podpisu cyfrowego i jego weryfikacja .....37

##### 1.4.2. Algorytmy podpisu cyfrowego .....39

##### 1.4.3. Podpis elektroniczny a podpis cyfrowy .....40

##### 1.4.4. Podpis elektroniczny w prawie polskim .....40

#### 1.5. Znacznik czasu .....42

#### 1.6. Bezpieczeństwo w kryptografii .....42

## **2. Fundamenty PKI .....44**

### **2.1. Cyfrowe certyfikaty .....46**

2.1.1. Wydawanie certyfikatu cyfrowego .....	47
2.1.2. Cykl życia certyfikatu .....	50
2.1.3. Certyfikaty X.509v.3 .....	50
2.2. Podstawowe komponenty PKI .....	53
2.2.1. Urząd Certyfikacji (CA) .....	54
2.2.2. Urząd Rejestracji (RA) .....	55
2.2.3. Repozytorium Certyfikatów (CR) .....	56
2.2.4. Jednostka końcowa (EE) .....	57
2.3. Funkcje PKI .....	58
2.4. Architektury PKI .....	63
2.4.1. Architektura hierarchiczna .....	64
2.4.2. Architektura rozproszonego zaufania .....	66
2.4.3. Zaufanie skoncentrowane na użytkowniku .....	67
2.5. ścieżka certyfikacji .....	68
2.6. Standardy PKI .....	69

### **3. PKI w praktyce .....71**

3.1. Bezpieczny dostęp do serwera – protokół SSL/TLS .....	72
3.2. Bezpieczna poczta elektroniczna .....	75
3.3. Bezpieczny zdalny dostęp do zasobów sieciowych .....	77
3.3.1. IPSec VPN .....	79
3.3.2. SSL VPN .....	81
3.4. Bezpieczne datowanie – TSP .....	82
3.4.1. Aplikacja FST Ricerca Time-Stamp Client .....	84
3.5. PKI w zastosowaniach mobilnych .....	85
3.5.1. Podpis elektroniczny przez 'komórkę' .....	86
3.5.2. SMS z e-podpisem .....	88

### **4. Praktyczna implementacja usług PKI w oparciu o platformę Windows Server 2003 .....89**

4.1. Instalowanie urzędu certyfikacji (CA) .....	90
4.2. Zarządzanie serwerem certyfikatów .....	93
4.3. Uzyskiwanie certyfikatów .....	94

4.4. Uwierzytelnianie w oparciu o certyfikaty – porównanie metod logowania z wykorzystaniem testowej strony WWW 98

**Zakończenie .....106**

**Bibliografia .....108**