

Charakterystyka infrastruktury elektronicznego

podpisu

Wstęp 4

Rozdział I. Podpis elektroniczny z technicznego punktu widzenia 6

- 1.1. Zagadnienia wstępne 6
 - 1.1.1. Zarys historyczny kryptografii 6
 - 1.1.2. Kryptografia symetryczna 8
 - 1.1.3. Kryptografia asymetryczna 11
- 1.2. PKI – Infrastruktura Klucza Publicznego 14
 - 1.2.1. Certyfikat i rola centrów certyfikacji 14
 - 1.2.1.1. Funkcje certyfikatu 19
 - 1.2.2. Architektura PKI 19
 - 1.2.3. Funkcje PKI 21
 - 1.2.4. Standardy PKI 24

Rozdział II. Geneza powstania podpisu elektronicznego 26

- 2.1. Historia powstania podpisu elektronicznego 26
 - 2.1.2. Pojęcie podpisu elektronicznego 26
 - 2.1.2.1. Podpis elektroniczny w USA 26
 - 2.1.2.2. Podpis elektroniczny w Unii Europejskiej 27
 - 2.1.2.3. Podpis elektroniczny w Polsce 28
 - 2.1.3. Rodzaje podpisu elektronicznego 30
 - 2.1.4. Funkcje podpisu elektronicznego 30
 - 2.1.5. Zasady działania podpisu elektronicznego 31

Rozdział III. Zastosowanie podpisu elektronicznego 34

- 3.1. Pobieranie certyfikatu 34
 - 3.1.1. Pobieranie certyfikatu głównego 34
- 3.2. Pobieranie certyfikatu własnego 36
- 3.3. Korespondencja elektroniczna 38
 - 3.3.1. Szyfrowanie poczty elektronicznej 38

3.4. Wykorzystanie podpisu elektronicznego w bankach 44

Rozdział IV. Problematyka zagrożeń podpisu elektronicznego 48

4.1. Kryptoanaliza 48

4.1.1. Atak siłowy 49

4.1.2. Kryptoanaliza różnicowa 49

4.1.3. Kryptoanaliza liniowa 50

4.1.4. Inne formy ataków 51

Rozdział V. Podpis elektroniczny w przepisach prawa 54

5.1. Podpis elektroniczny w polskiej ustawie 54

5.2. Podmioty świadczące usługi certyfikacyjne 56

5.3. Oświadczenie woli 61

5.4. Nadzór państwa 63

Zakończenie 67

Bibliografia 70

Spis tabel 74

Spis rysunków 75