

Technologie podpísów cyfrowych – funkcjonowanie i zastosowanie

Podpisy cyfrowe.

3.1. Tworzenie podpisu cyfrowego	25
3.2. Zasada działania	26
3.3. Przyszłość podpisów cyfrowych.....	30
3.4. Co nie jest podpisem cyfrowym.....	30
3.5. Wady.....	31
3.6. Podstawowe rodzaje ataków na podpis cyfrowy	32
3.7. Protokoły związane z podpisami.....	33
3.7.1. Slepe podpisy	33
3.7.2. Kanał podprogowy	33
3.7.3. Podpisy niezaprzeczalne.....	34
3.8. Znacznik czasu	34
3.8.1. Skrót Kryptograficzny SHA1	35
3.8.2. Wiarygodny Czas	36
3.8.3. Kwalifikowany Podpis Elektroniczny.....	36
3.8.4. Oznaczanie Czasem Archiwizowanych Danych	36

Rozdział 4

Certyfikaty cyfrowe

4.1. Uzyskiwanie certyfikatu	38
4.2. Struktura certyfikatu.....	43
4.2.1. Struktura certyfikatu w notacji ASN.1:	43
4.2.2. Pola podstawowe.....	44
4.2.3. Rozszerzenia certyfikatu	46
4.3. Profile certyfikatu	48
4.4. Inne profile certyfikatu.....	49
4.5. Cztery stany certyfikatów	50
4.6. Wiarygodność usług certyfikacji i uwierzytelniania	51

Rozdział 5

Infrastruktura klucza publicznego – PKI.

5.1. Podstawowe elementy i funkcje systemu PKI.....	56
5.2. Hierarchia urzędów certyfikatów.....	60
5.3. Weryfikowanie certyfikatów przy wykorzystaniu	

Katalogu.....62

5.4. Alternatywne schematy weryfikacji62

Rozdział 6

Transakcje internetowe a pospis cyfrowy.

6.1. Model elektronicznego systemu płatności.....64

6.2. Wymagania w zakresie bezpieczeństwa66

6.2.1. Wiarygodność i autoryzacja66

6.2.2. Poufność67

6.2.3. Dostępność i niezawodność.....68

6.3. Przegląd technologii.....68

6.3.1. Tryby Transakcji Online i Offline68

6.3.2. Niezawodność sprzętu komputerowego69

6.3.3. Kryptografia70

6.3.4. Anonimowość płatnika.....72

6.4. Mikropłatności74

6.5. Standardy76

6.6. Systemy obecnie wykorzystywane78

6.7. Model bezpiecznej sprzedaży.....79

6.8. Protokół SSL81

6.9. Protokół S-HTTP82

6.10. Protokół iKP firmy IBM.....82

6.11. Karty wirtualne84

Podsumowanie.....86

Załącznik słownik pojęć.....89

Literatura.....91