Infrastruktura klucza publicznego – PKI

ADAM ZIĘTA 126910

Plan prezentacji

- Historia
- Certyfikaty cyfrowe i metody szyfrowania
- Struktura PKI
- Funkcje i zastosowania PKI
- Standardy PKI

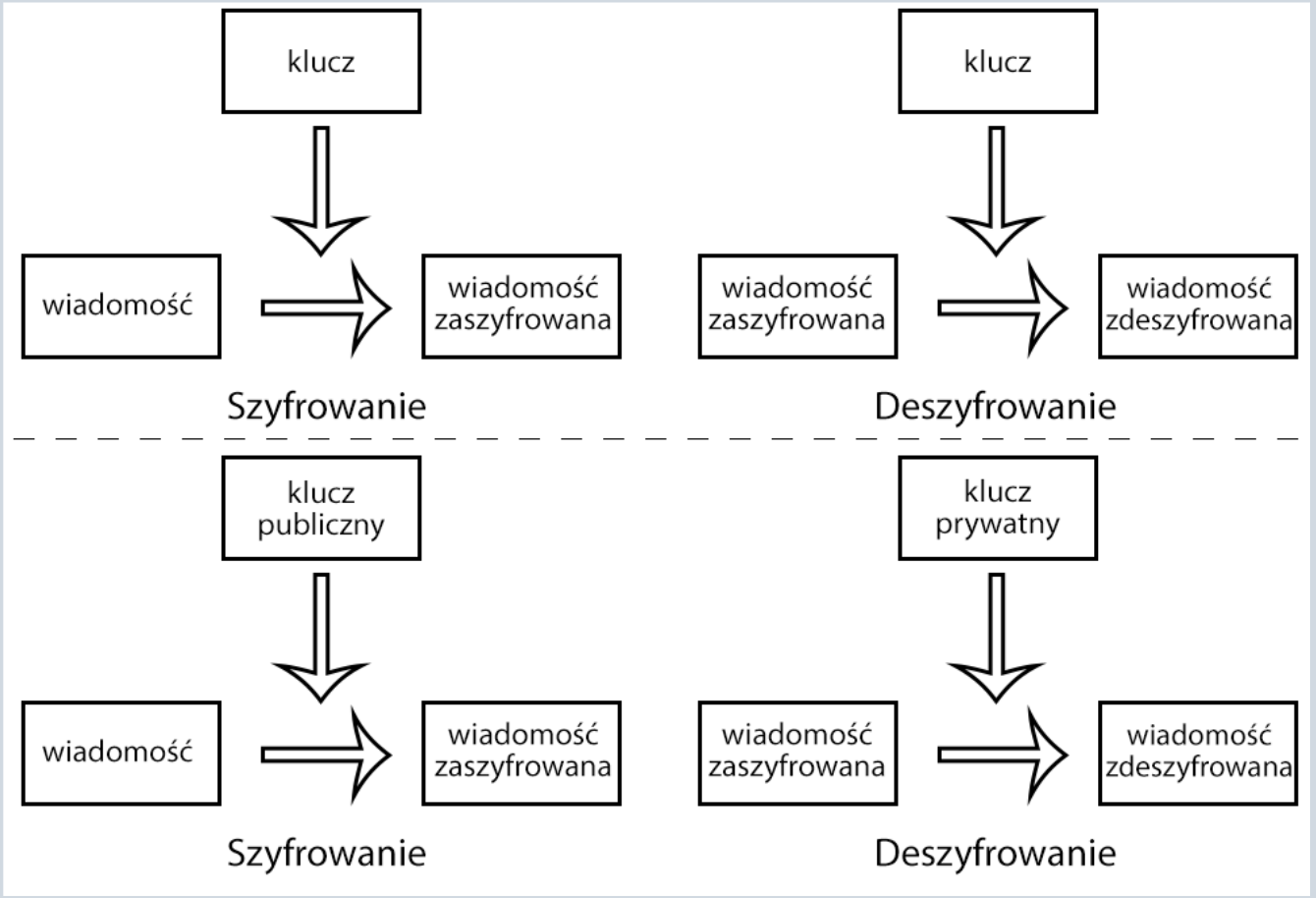
Historia

- 1976 rok
- Whitfield Diffie, Martin Hellman, Ron Rivest, Adi Szamir, Leonard Adleman
- Taher Elgamal, Netscape
- American Bar Association

Krótka powtórka

Metody szyfrowania

- Symetryczne
- Asymetryczne



Krótka powtórka c.d.

Certyfikaty cyfrowe – to elektroniczne zaświadczenie za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowywane do określonej osoby i potwierdzają tożsamość tej osoby.

Infrastruktura klucza publicznego

Infrastruktura służąca do zarządzania cyfrowymi certyfikatami i kluczami szyfrującymi dla osób, programów i systemów.

Struktura PKI

- Urząd Rejestracji (*Registration Authority - RA*)
- Urząd Certyfikacji (*Certification Authority – CA*)
- Repozytorium certyfikatów
- Użytkownicy końcowi (*End Entity*)

Funkcje

- Rejestracja
- Certyfikacja
- Generacja, odnawianie i odzyskiwanie kluczy
- Certyfikacja wzajemna
- Odwołanie certyfikatu

Zastosowania

- Bezpieczna poczta

- Wirtualne sieci prywatne VPN

- E-commerce

- Zapewnieniu bezpieczeństwa na witrynach internetowych, urządzeniach i aplikacjach klienta

Standardy PKI

- PKIX
- X.509
- PKCS (*Public Key Cryptography Standard)*
- XML Signature
- PN-ISO/IEC 9796
- ISO/IEC 27001:2005

Dziękuje za uwagę!