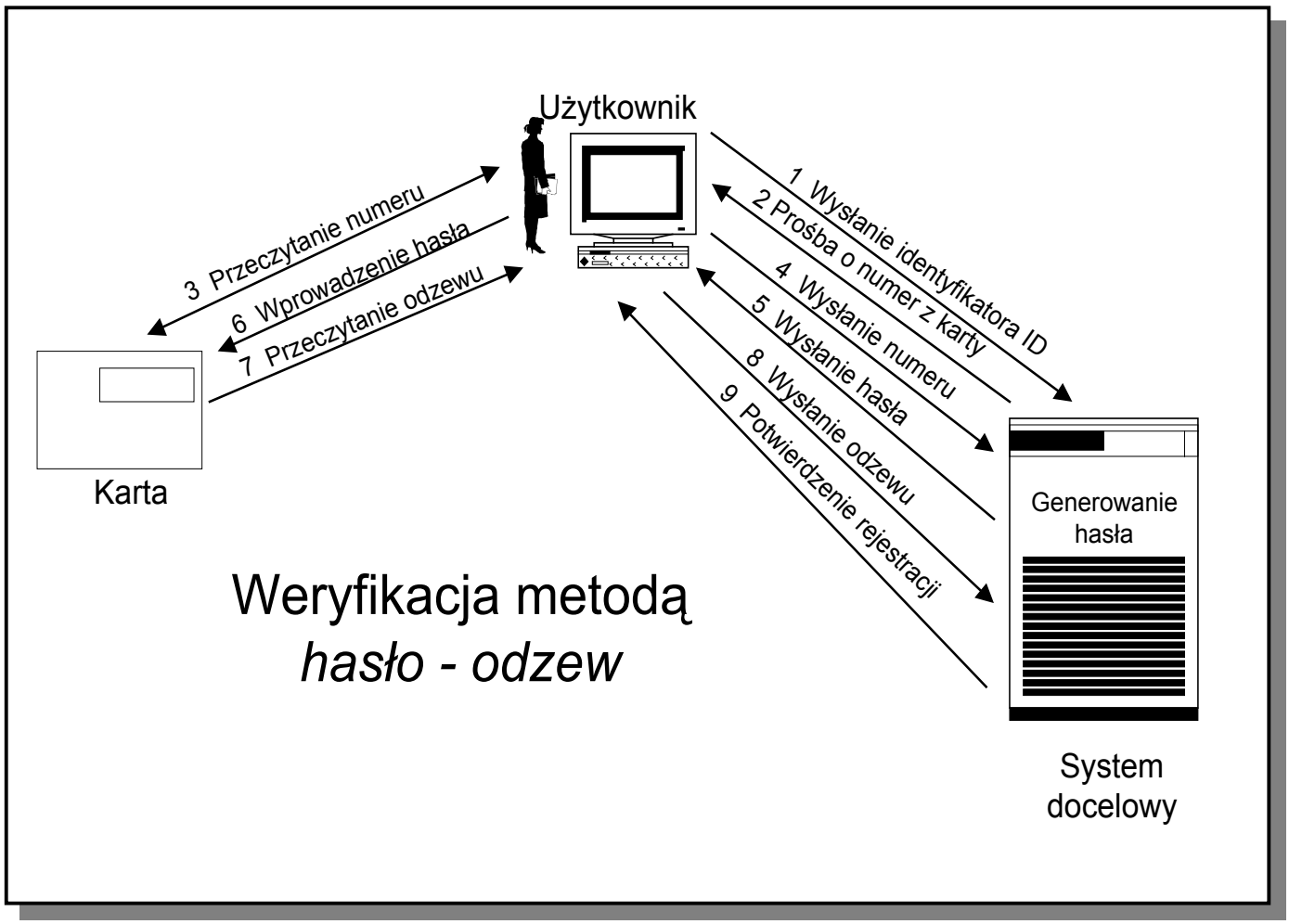
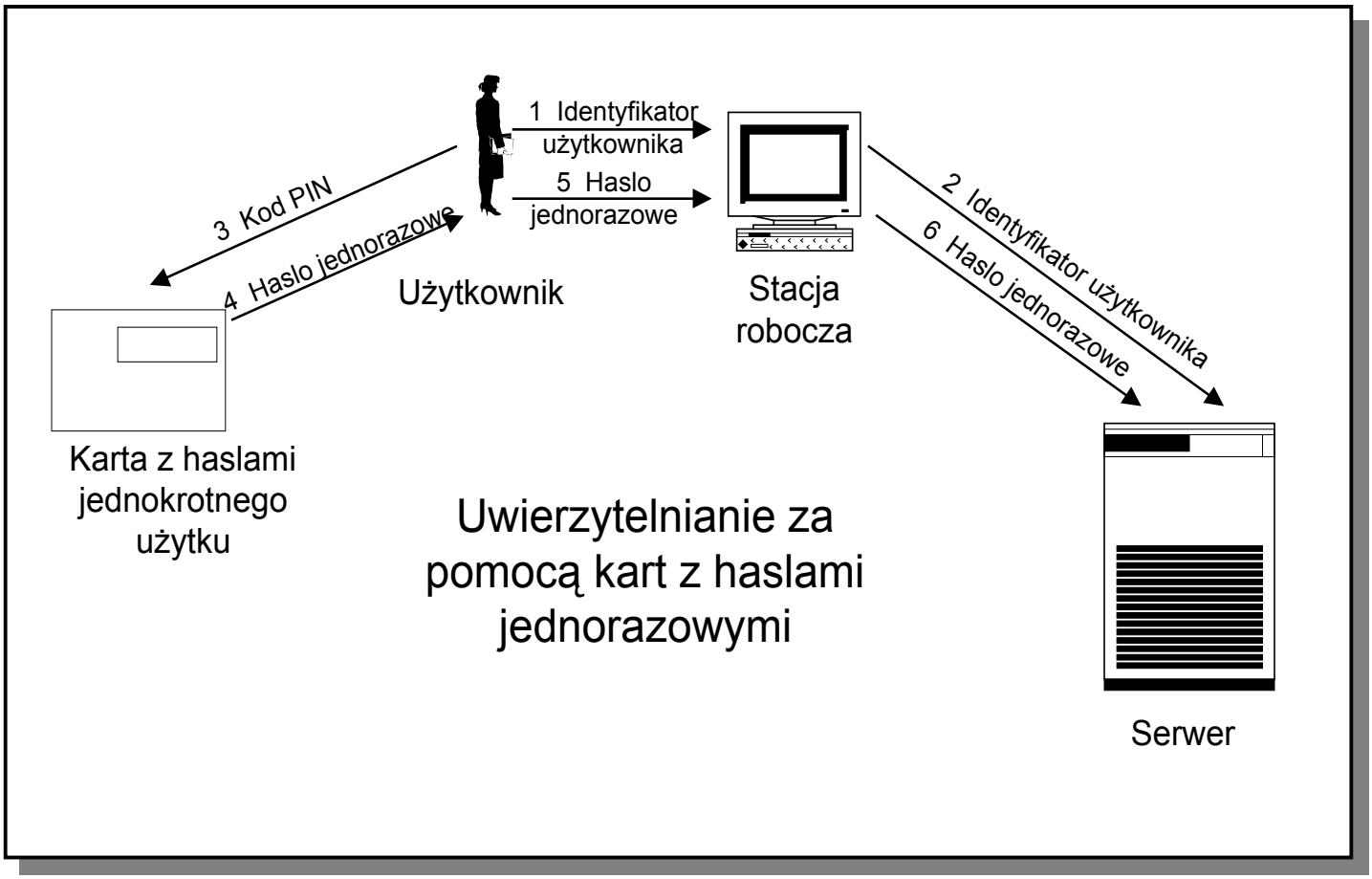
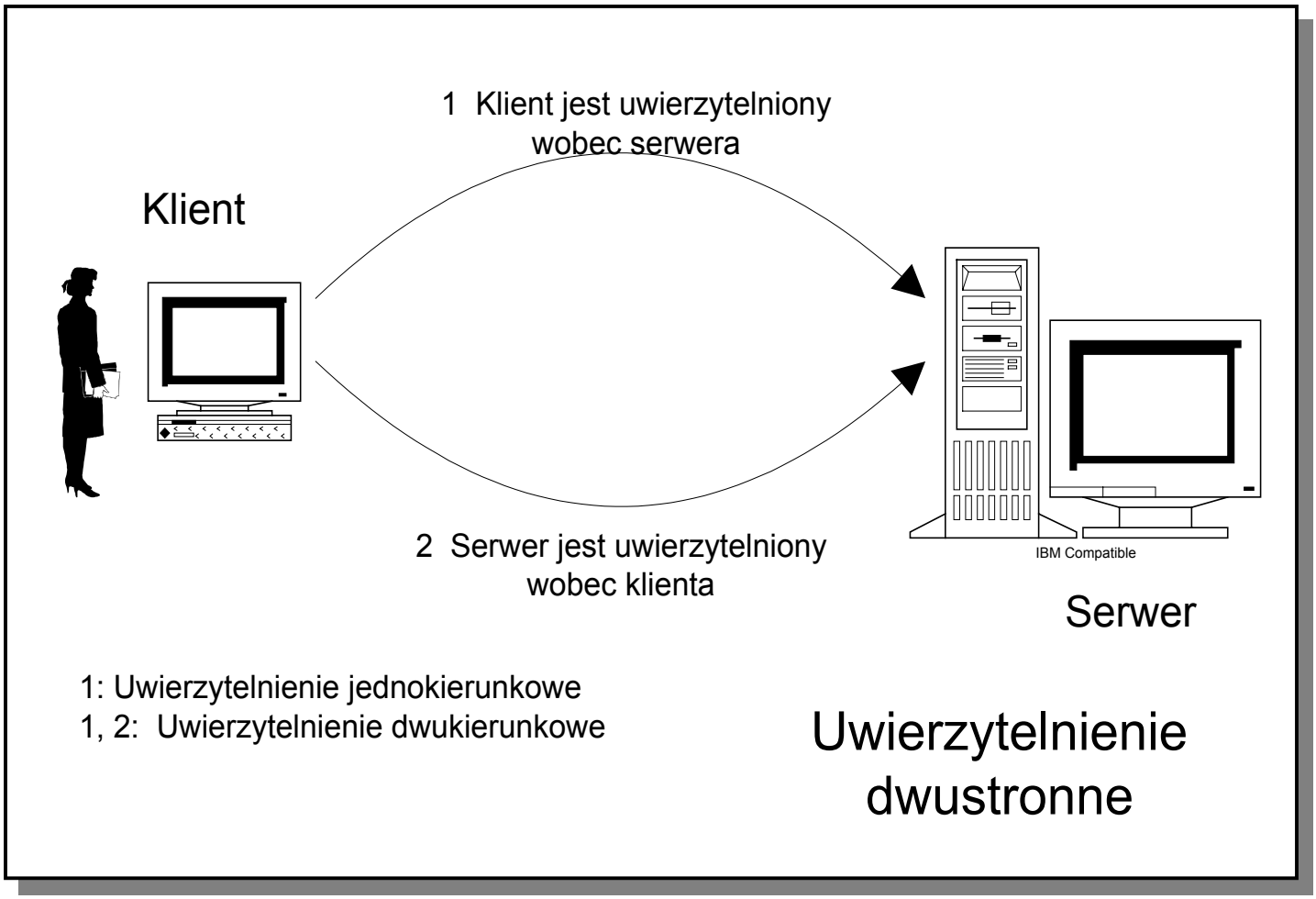

Użytkownik
1 Wysłanie identyfikatora ID
2 Prośba o numer z karty
3 Przeczytanie numeru
4 Wysłanie numeru
5 Wysłanie hasła
6 Wprowadzenie hasła
7 Przeczytanie odzewu
8 Wysłanie odzewu
9 Potwierdzenie rejestracji
Karta
Generowanie hasła
System docelowy
Weryfikacja metodą
hasło - odzew

Ochrona haseł:

- Nadzorowanie haseł (wybór, pielęgnacja).
  - Komunikaty systemowe
  - Wprowadzanie hasła
  - Ograniczanie ilości prób rejestracji
  - Starzenie się haseł
  - Systemy z dwoma hasłami
  - Minimalna długość hasła
  - Blokowanie konta użytkownika
  - Ochrona hasła administratora
  - Generowanie hasła przez system
- Zabezpieczanie przed odgadnięciem poprzez odrzucanie zbyt łatwych haseł.
  - Sprawdzanie bierne
  - Sprawdzanie czynne
- Bezpieczne przechowywanie haseł.


1 Identyfikator użytkownika
5 Haslo jednorazowe
3 Kod PIN
4 Haslo jednorazowe
2 Identyfikator użytkownika
6 Haslo jednorazowe
Użytkownik
Stacja robocza
Karta z haslami jednokrotnego użytku
Uwierzytelnianie za pomocą kart z haslami jednorazowymi
Serwer


1 Klient jest uwierzytelniony wobec serwera
Klient
2 Serwer jest uwierzytelniony wobec klienta
IBM Compatible
Serwer
1: Uwierzytelnienie jednokierunkowe
1, 2: Uwierzytelnienie dwukierunkowe
Uwierzytelnienie dwustronne

Struktura certyfikatu X.509

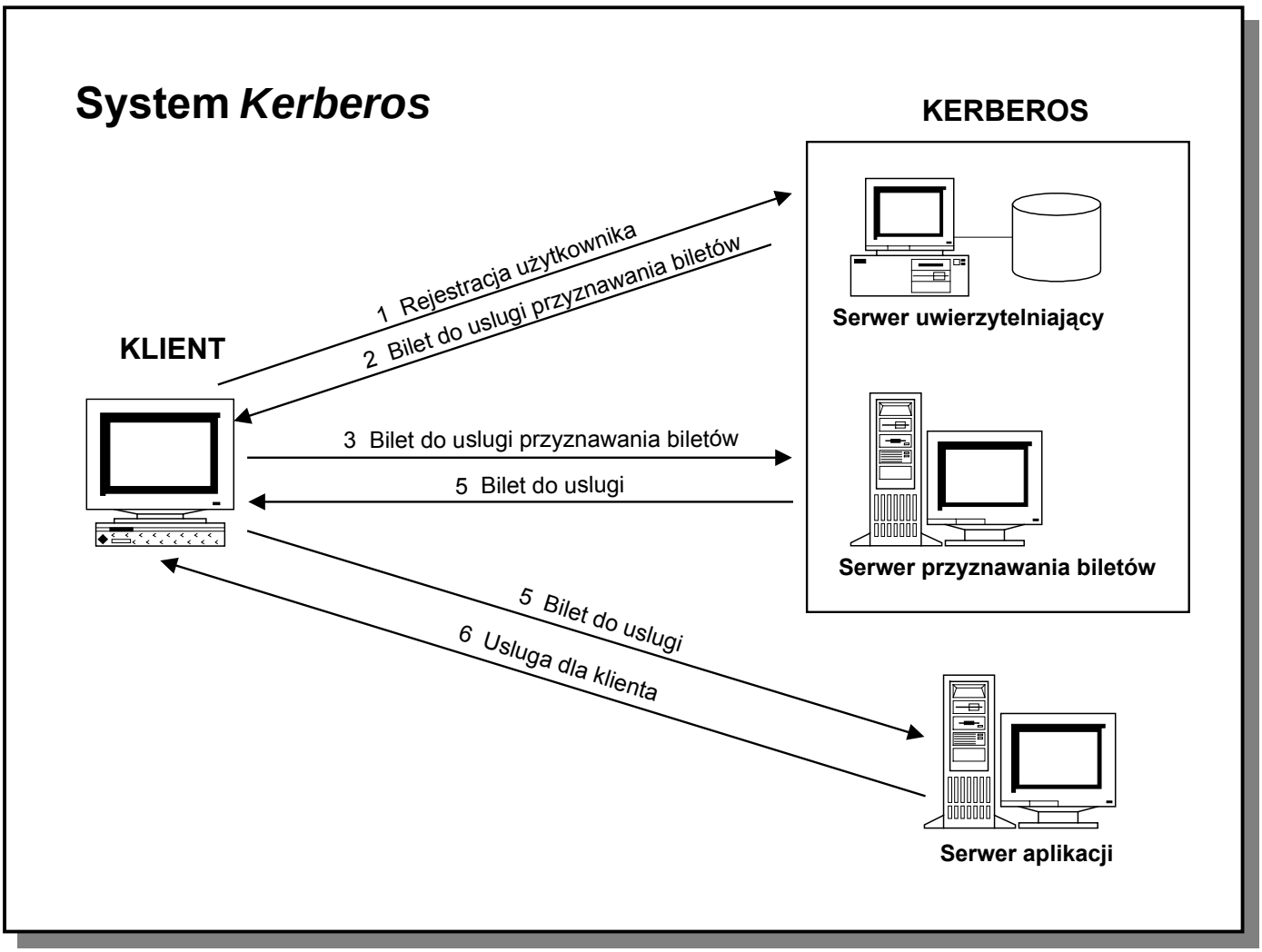
- **Numer wersji**
- **Numer seryjny**
- **Identyfikator algorytmu**
- **Identyfikator wystawcy**
- **Okres ważności**
- **Użytkownik certyfikatu**
- **Informacja o kluczu publicznym**
- **Podpis cyfrowy**

Uwierzytelniania stosowane w bankach internetowych w Polsce

Lukas e-Bank - Token SecureID
producent: RSA Security

ePKO BP - token ActiveCard Plus
producent: Active Card

TelePekao24, WBK24 - Token DigiPass 300
producent: Vasco


System *Kerberos*
KERBEROS
Serwer uwierzytelniający
KLIENT
1 Rejestracja użytkownika
2 Bilet do uslugi przyznawania biletów
3 Bilet do uslugi przyznawania biletów
5 Bilet do uslugi
Serwer przyznawania biletów
5 Bilet do uslugi
6 Usluga dla klienta
Serwer aplikacji

System *Kerberos*

C1>AS: $C1, TGS, T_2$

AS>C1: $\{TGS, K_{C1,TGS}, T_2, L_2, \{TGT_{C1,TGS}\} K_{AS,TGS} \} K_{C1}$

C1>TGS: $\{S1, C1, T_3\} K_{C1,TGS}, \{TGT_{C1,TGS}\} K_{AS,TGS}$

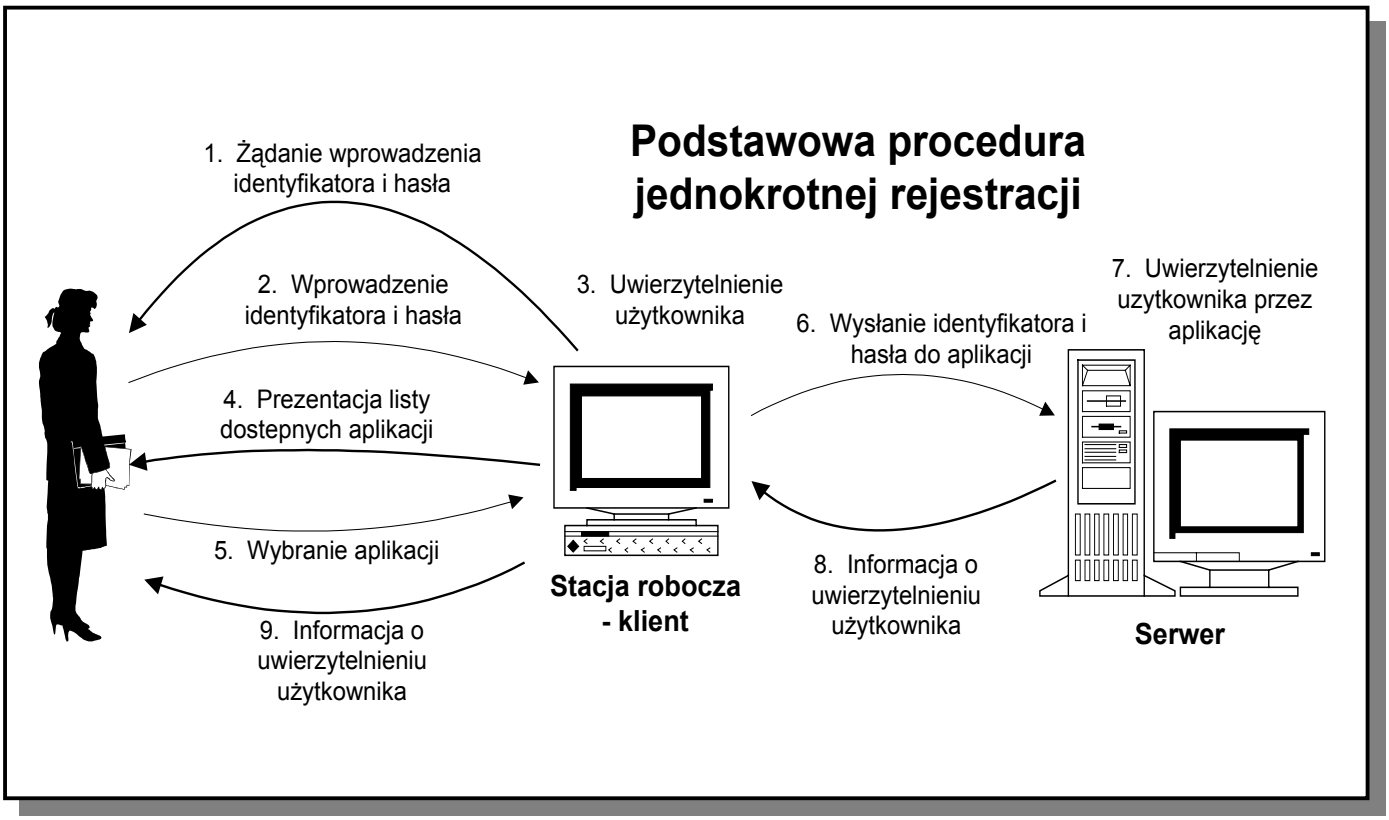
TGS>C1: $\{ K_{C1,S1}, S1, T_4, \{B_{C1,S1}\}K_{S1,TGS} \}K_{C1,TGS}$

C1>S1: $\{B_{C1,S1}\}K_{S1,TGS}, \{ C1, T_5\}K_{C1,S1}$

S1>C1: $\{ T_5 + 1\} K_{C1,S1}$

System *Kerberos* - atrybuty biletów

- **Bilety początkowe** (flaga INITIAL).
- **Bilety nieważne** (flaga INVALID)
- **Bilety odnawialne** (flaga RENEWABLE)
- **Bilety postdatowane** (flagi MAY_POSTDATE, POSTDATED)
- **Bilety upełnomocniające się i upełnomocnione** (flagi PROXIABLE i PROXY)
- **Bilety przekazywalne** (flagi FORWARDABLE i FORWARD)


Podstawowa procedura jednokrotnej rejestracji
1. Żądanie wprowadzenia identyfikatora i hasła
2. Wprowadzenie identyfikatora i hasła
3. Uwierzytelnienie użytkownika
4. Prezentacja listy dostepnych aplikacji
5. Wybranie aplikacji
6. Wysłanie identyfikatora i hasła do aplikacji
7. Uwierzytelnienie uzytkownika przez aplikację
8. Informacja o uwierzytelnieniu użytkownika
9. Informacja o uwierzytelnieniu użytkownika
Stacja robocza - klient
Serwer

Literatura:

1) V. Ahuja. *Network & Internet Security*. Academic Press, Inc, 1996.
2) P. Brown. *ICL Extends Access Manager to Sun Platforms.* Communications Week. Oct. 1994.
3) D. A. Curry. *UNIX System Security: A Guide for Users and System Administrators.* Addison-Wesley 1992.
4) J. Edwards. *Single Sign-on Technologu Streamlines Network Access.* Software Magazine. Nov. 1993.
5) M. Hurwicz. *Under Lock and Key*. Special Report, LAN Magazine. March 1995.
6) J. T. Johnson, K. Tolly. *Token Authentication: The Safety Catch.* Data Communication, May 1995.
7) L.Klander. *Hacker Proof*. Jamsa Press, 1997 (*tłum.* MIKOM 1998).
8) D. V. Klein. *Foiling the Cracker: A Survey of, and Improvements to, Password Security.* UNIX Security Workshop, Portland 1990.
9) J. Kohl, B. Neuman. *The Kerberos Network Authentication Service*. RFC 1510. Sep. 1993.
10) S. J. Lunt. *Experiences with Kerberos.* UNIX Security Workshop USENIX Assoc. Portland 1990.
11) R. Morris, K. Thompson. *Password Security: A Case History*. Comm. Of the ACM, v22, n.11, Nov. 1979.
12) National Computer Security Center, *Department of Defence Password Management Guideline.* CSC-STD-002-85.
13) R. M. Needham, M. D. Schroeder. *Using Encryption for Authentication in Large Networks of Computers*. Communications of the ACM, v. 21, n. 12, Dec 1978.
14) T.M. Raleigh, R.W. Underwood. *CRACK: A Distributed Password Advisor.* UNIX Security Workshop. Portland 1988.
15) D. Russell, G.T. Gangemi. *Computer Security Basics*. O'Reilly&Associates, 1991.
16) E. H. Spafford. *Observing Reusable Password Choices.* Proc. 1992 Usenix Security Workshop, 1992.
17) W. Stallings. *Network and Internetwork Security: Principles and Practice*. Prentice Hall 1995.
18) J. G. Steiner, C. Neuman, J. I. Schiller. *Kerberos: An Authentication Service for Open Network Systems.* Proc. of the Winter 1988 USENIX Conf. Feb. 1988.