Bezpieczny dostęp do usług zarządzania danymi w systemie Laboratorium Wirtualnego

Poznańskie Centrum Superkomputerowo Supersieciowe:

M.Lawenda, M.Wolski, N.Majer, C.Mazurek, M.Stroiński

Politechnika Łódzka Centrum Komputerowe:

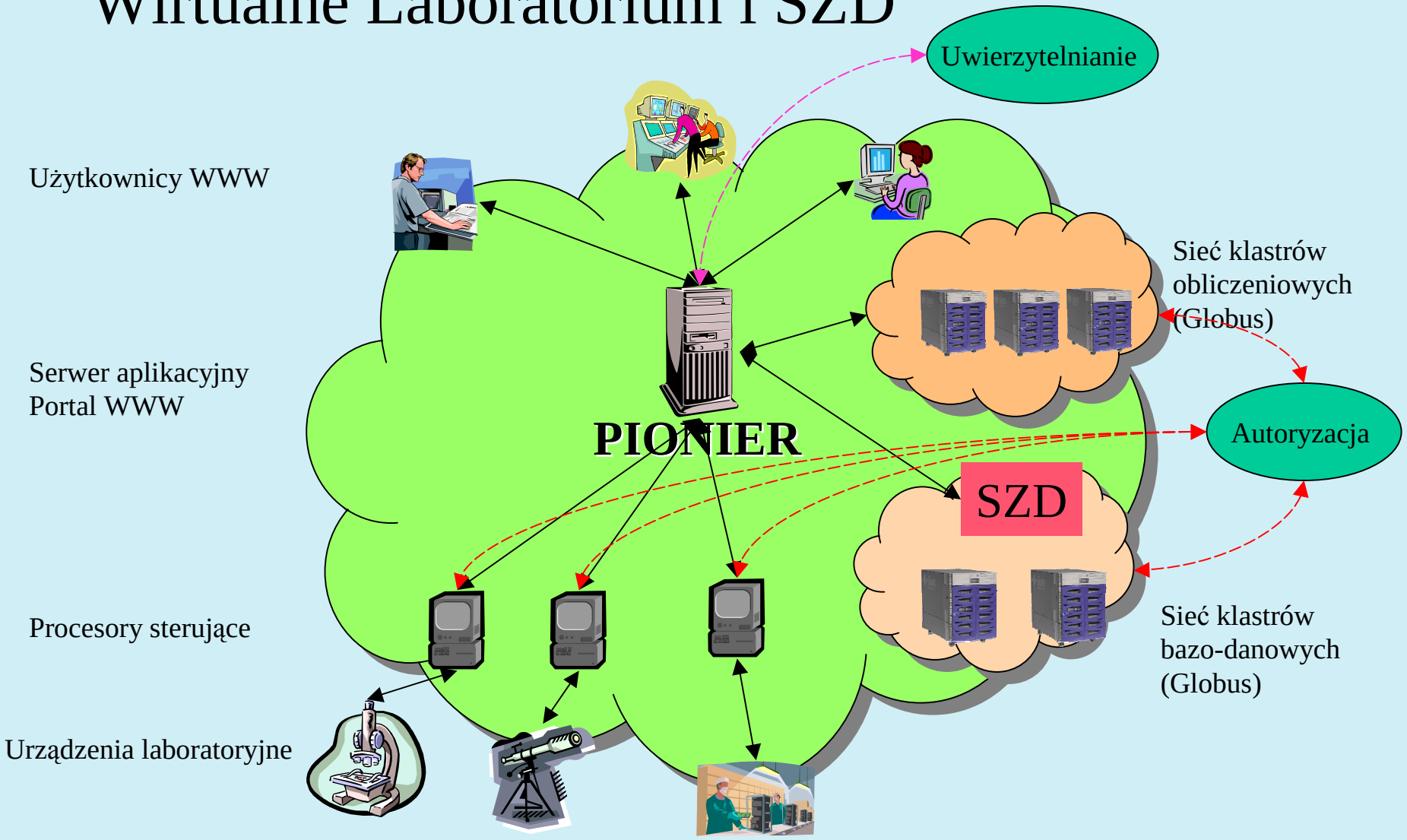
P.Szychowski, M.Kopeć

PIONIER 2004

Agenda

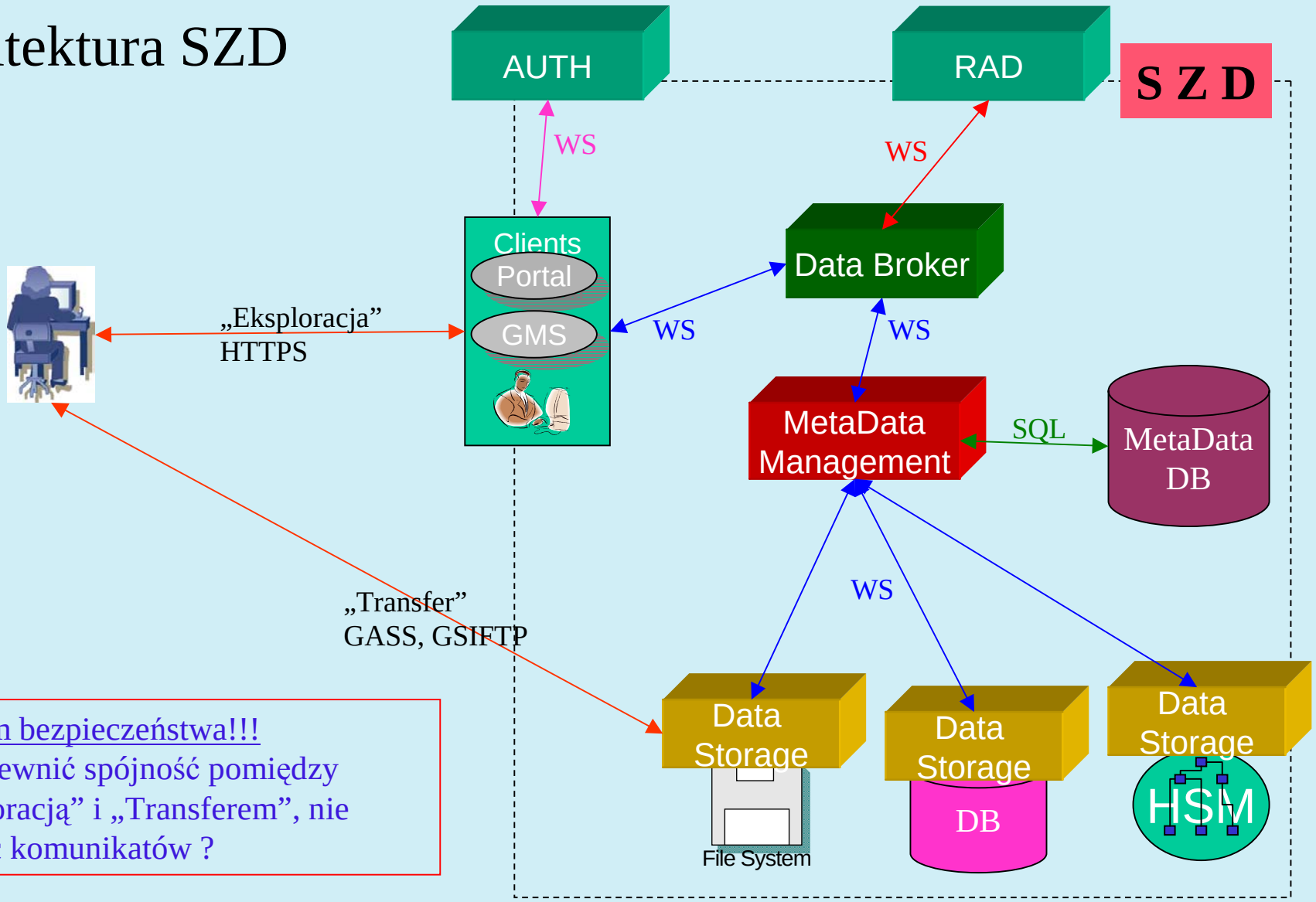
- Ogólna architektura Systemu Zarządzania Danymi
- Warstwa bezpieczeństwa w projekcie SGIgrid
- Rozwiązanie uwierzytelniania i autoryzacji w SZD Wirtualnego Laboratorium

Wirtualne Laboratorium i SZD



PIONIER 2004

Architektura SZD



Problem bezpieczeństwa!!!
Jak zapewnić spójność pomiędzy „Eksploracją” i „Transferem”, nie mnożąc komunikatów ?

Bezpieczeństwo w gridach – Wirtualna Organizacja.

Cechy funkcjonalne:

- Uwierzytelnianie i autoryzacja:
  - wiadomo kto i co robi
- Poufność i integralność danych
  - dane są niewidoczne dla postronnych i odporne na nieuprawnioną modyfikację
- Spójność operacji
  - operacje na rozproszonych zasobach mogą być wykonywane w ustalonym porządku i czasie

Cechy technologiczne:

- Wielopoziomowość zabezpieczeń (AA – autentykacja/autoryzacja)
- Scentralizowana autentykacja AUTH i autoryzacja RAD (CAS – Comunity Authorization Service)
- Silna kryptografia (security, non-repudition)
- Zasada SSO (Single Sign-Only)

GSI – Globus Security Infrastructure uznany standard bezpieczeństwa

- GSI jest technologią udostępnioną w Globus Toolkit:
  - Kryptografia PKCS
  - Delegacja uprawnienia (Certyfikat Proxy, który służy do okazania w zastępstwie własnego certyfikatu X.509)
  - Transfer plików GASS i GSIFTP oparty na SSLv3
- GSI GT2 różni się istotnie od GSI GT3

GSI GT2 i GT3 - porównanie

- GSI GT2
  - Główne cechy:
    - Autentykacja opiera się o zawarość pliku *grid-mapfile*
    - Autoryzacja opiera się o system lokalnego serwera
  - Wady:
    - system jest trudno skalowalny
    - system autoryzacji VO jest zależny od administratora lokalnego systemu

- GSI GT3
  - Główne cechy:
    - Autentykacja i autoryzacja opiera się o zewnętrzny system CAS (najlepiej centralny dla VO)
    - Jest wykorzystane pole PCI (Proxy Certificate Information – rozszerzenie X.509)
  - Zalety:
    - System CAS jest Gridserwisem („Webserwisem”), dzięki czemu jest uniwersalny,
    - rozwiązanie dobrze skalowalne

Certyfikat proxy (credential)

- Standard IETF PKIX (na razie draft)
- Używanie proxy wzmacnia bezpieczeństwo, ponieważ stosując krótkoterminowe klucze do zwykłych operacji w gridzie, ograniczmy częstotliwość wykorzystania rzeczywistego klucza prywatnego (to oznacza mniejszą szansę kompromitacji klucza rzeczywistego)
- Certyfikat proxy pozwala zrealizować postulat SSO ponieważ jego użycie nie wymaga podawania hasła do klucza.
- Trzy rodzaje certyfikatów proxy:
  - Full delegation (GT2 i GT3)– umożliwia wyłącznie identyfikację,
  - Restricted delegation (GT3) – pozwala załączyć kontekstową politykę (PCI), która podlega weryfikacji przez CAS
  - No delegation (GT3) – komunikat żądania dodatkowych praw od CAS (na razie nie ma implementacji)

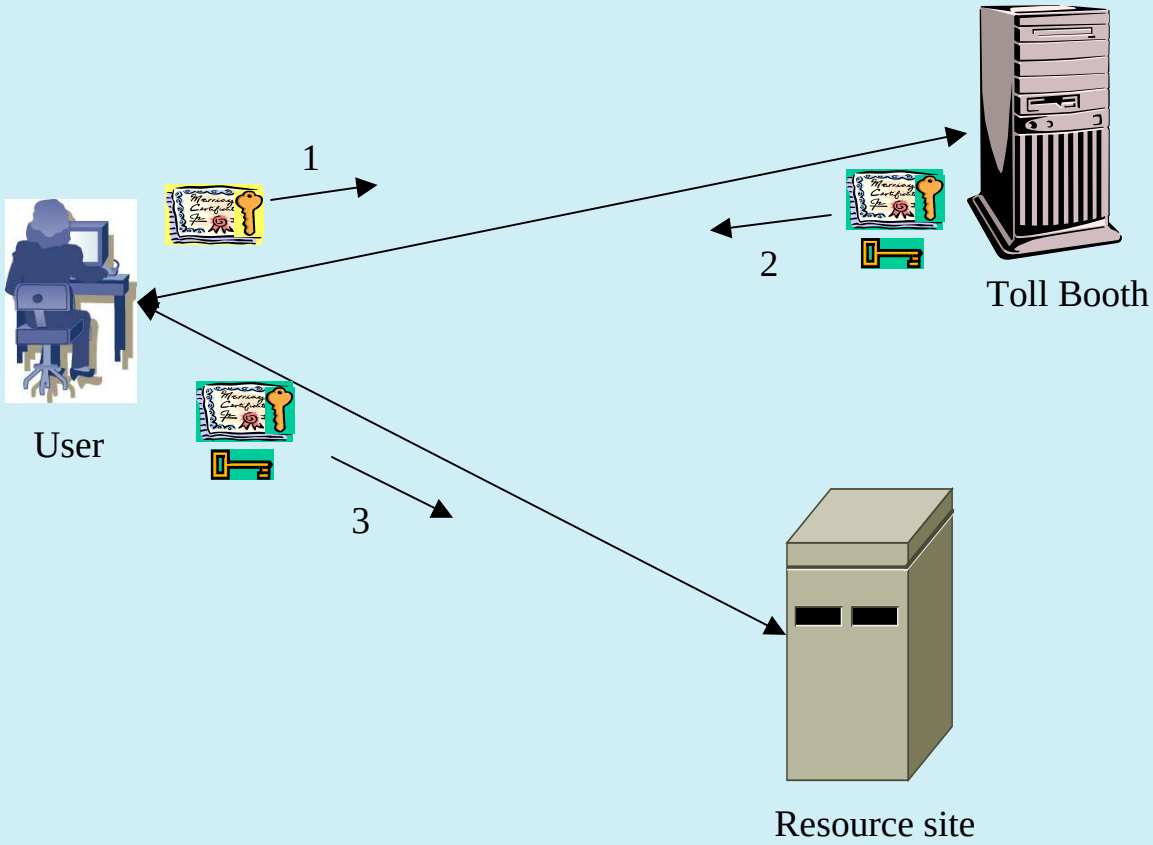
System bezpieczeństwa SGIgrid

- Centralny system uwierzytelniania (AUTH) będący jednocześnie wystawcą i repozytorium certyfikatów proxy
- Centralny system autoryzacji RAD (Resource Access Decision)
  - TAK/NIE = f (*userID*, *action*, *resource*)
- GSI GT2 – algorytm biletowy (*ticket*) + dynamiczny „grid-mapfile”

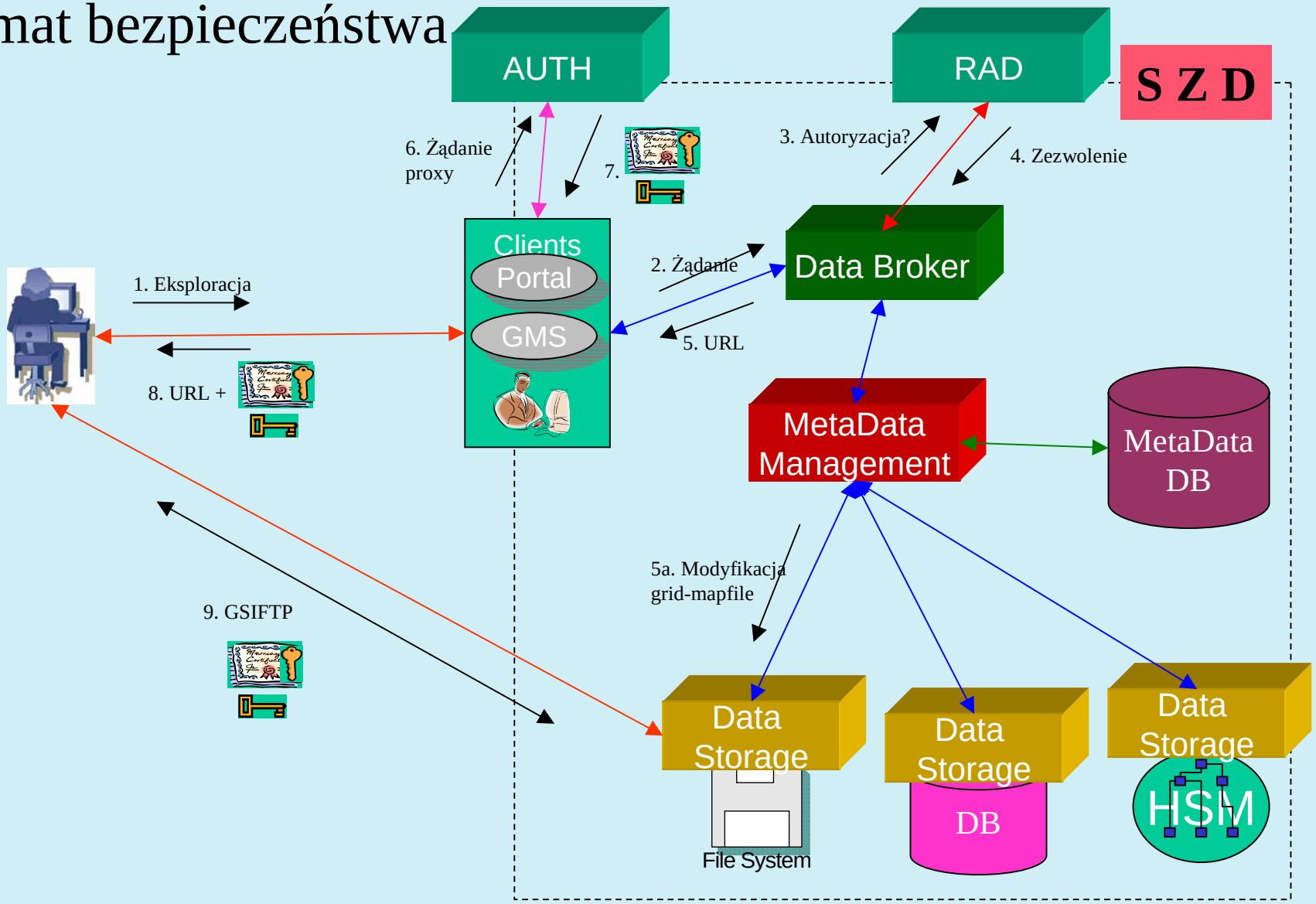
Algorytm biletowy dostępu do zasobu

- Algorytm biletowy (*ticket*) jest powszechnie znany z życia codziennego:
  - Kino - kupujemy bilet w kasie, który upoważnia do wejścia na salę filmową,
  - Stok narciarski – kupujemy impulsy do karty chipowej, które umożliwiają przejście przez bramkę do wyciągu.

Ogólny algorytm biletowy oparty na certyfikacie



Schemat bezpieczeństwa SZD



Podsumowanie

- Algorytm biletowy jest bardzo dobry – ekonomiczny, skalowalny, bezpieczny.
- Aby zrealizować bilety w oparciu o GSI GT2, z uwagi na brak obsługi rozszerzenia PCI, trzeba:
  - albo modyfikować serwery (GridFTP, GASS, GRAM itd..),
  - albo zaimplementować dynamiczne zarządzanie grid-mapfile.
  - albo pogodzić się z brakiem ponownej autoryzacji na poziomie zasobu.
- Bilety łatwo i w naturalny sposób można wdrożyć w GSI GT3:
  - obsługa polityki PCI w certfyfikatach proxy.