Rozproszony portal społecznościowy

Założenia, architektura i bezpieczeństwo

inż. Marcin Tunia

opiekun: prof. dr hab. inż. Zbigniew Kotulski

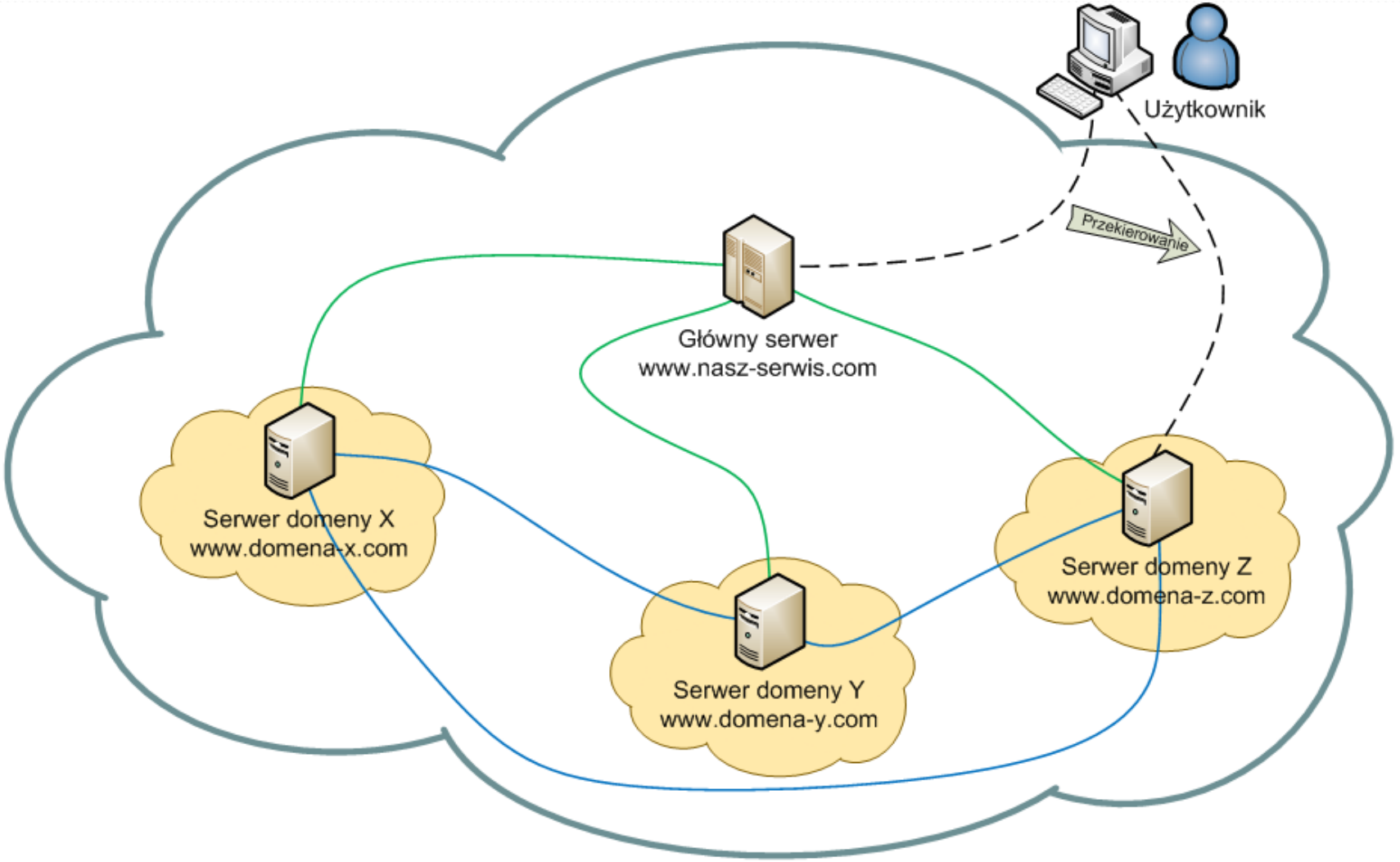
Plan prezentacji

- Założenia projektu
- Opis architektury
  - Role elementów
  - Role styków
  - Zalety rozwiązania
- Przypadek użycia
- Bezpieczeństwo
  - Środki bezpieczeństwa
  - Zagrożenia i obrona
- Narzędzia
- Plan dalszych działań

Założenia

- Portal społecznościowy (do wymiany multimediów)
  - Uproszczona wersja – wymiana danych tekstowych
- Brak zcentralizowanej bazy danych dla wszystkich użytkowników
- Wiele domen obsługujących użytkowników
- Wspólny serwer do zarządzania zgłoszeniami
- Serwer nie ma dostępu do danych użytkowników
- Modularność – możliwość dynamicznego dołączania nowych domen

Architektura



Domeny

- Posiadają własną politykę udostępniania na zewnątrz i wewnątrz domeny
- Użytkownicy ufają administratorowi swojej domeny, np.:
  - Uczelnia
  - Pracodawca
  - Prywatna domena
  - Domena komercyjna (związana z reklamą)

- Wszystkie dane przechowywane wewnątrz domeny
- Użytkownicy logują się do swojej domeny
- Legitymują się certyfikatem
- Możliwość logowania się przez domenę a nie przez serwer

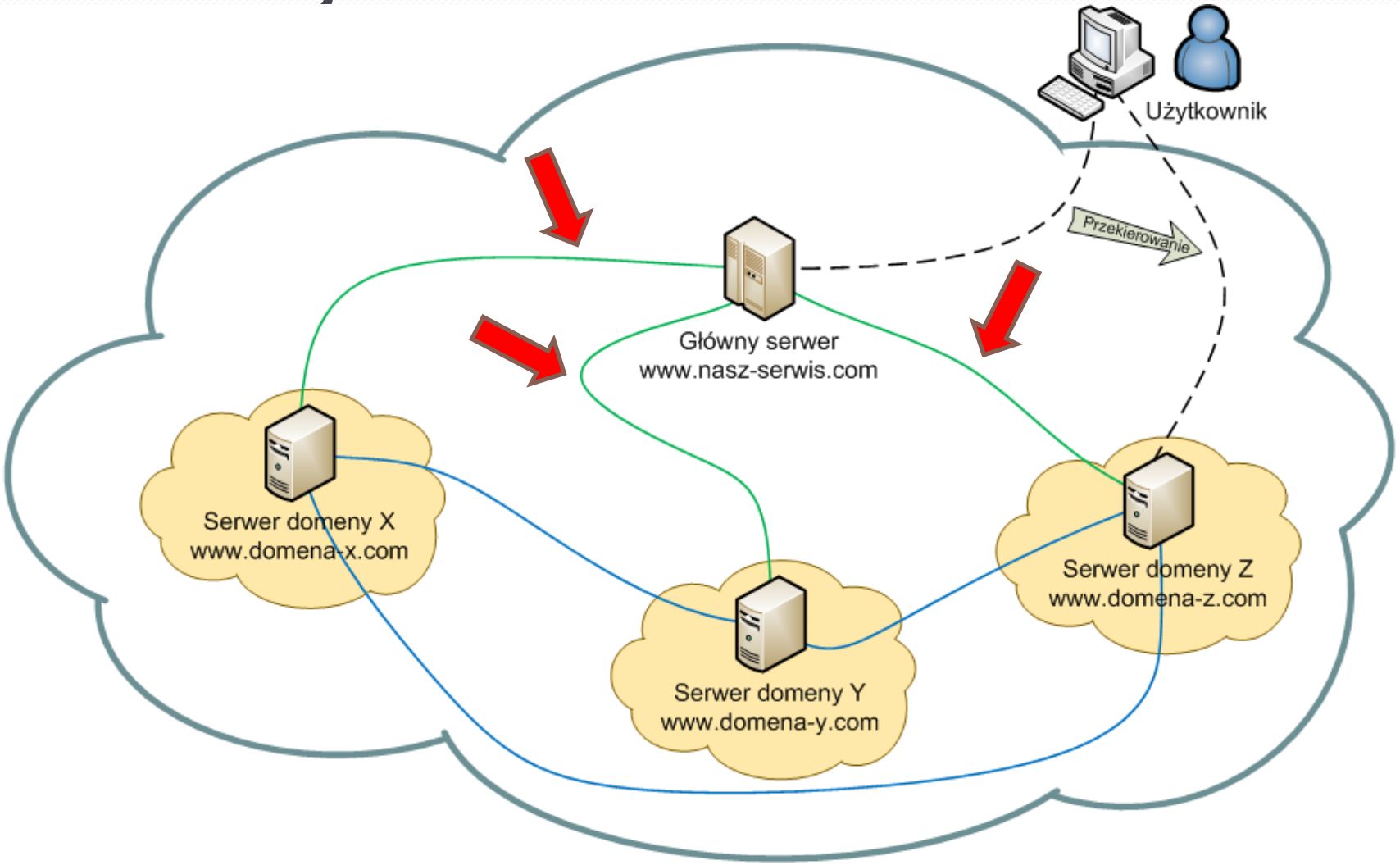
Główny serwer

- Obsługuje przychodzące zapytania o domenę użytkownika (lub dostępne domeny)
- Zwraca adres domeny
- Przechowuje loginy użytkowników i przypisane mu domeny
- Przechowuje dane domen podłączonych do systemu
  - Adres IP/www
  - Nazwa
  - Informacje ogólne
  - Politykę udostępniania (co udostępnia domena na zewnątrz)
  - Czy jest aktywna?
  - Kiedy ostatnio była aktywna?

Zalety rozwiązania

- Dane wszystkich użytkowników nie są przechowywane i przetwarzane przez jeden podmiot
- Elastyczność wyboru zaufanej domeny
- Dywersyfikacja polityk bezpieczeństwa
- Dla użytkownika system wygląda jak zcentralizowany system (serwer jako pierwszy punkt kontaktu)
- Modularność (łatwość stworzenia własnej domeny)

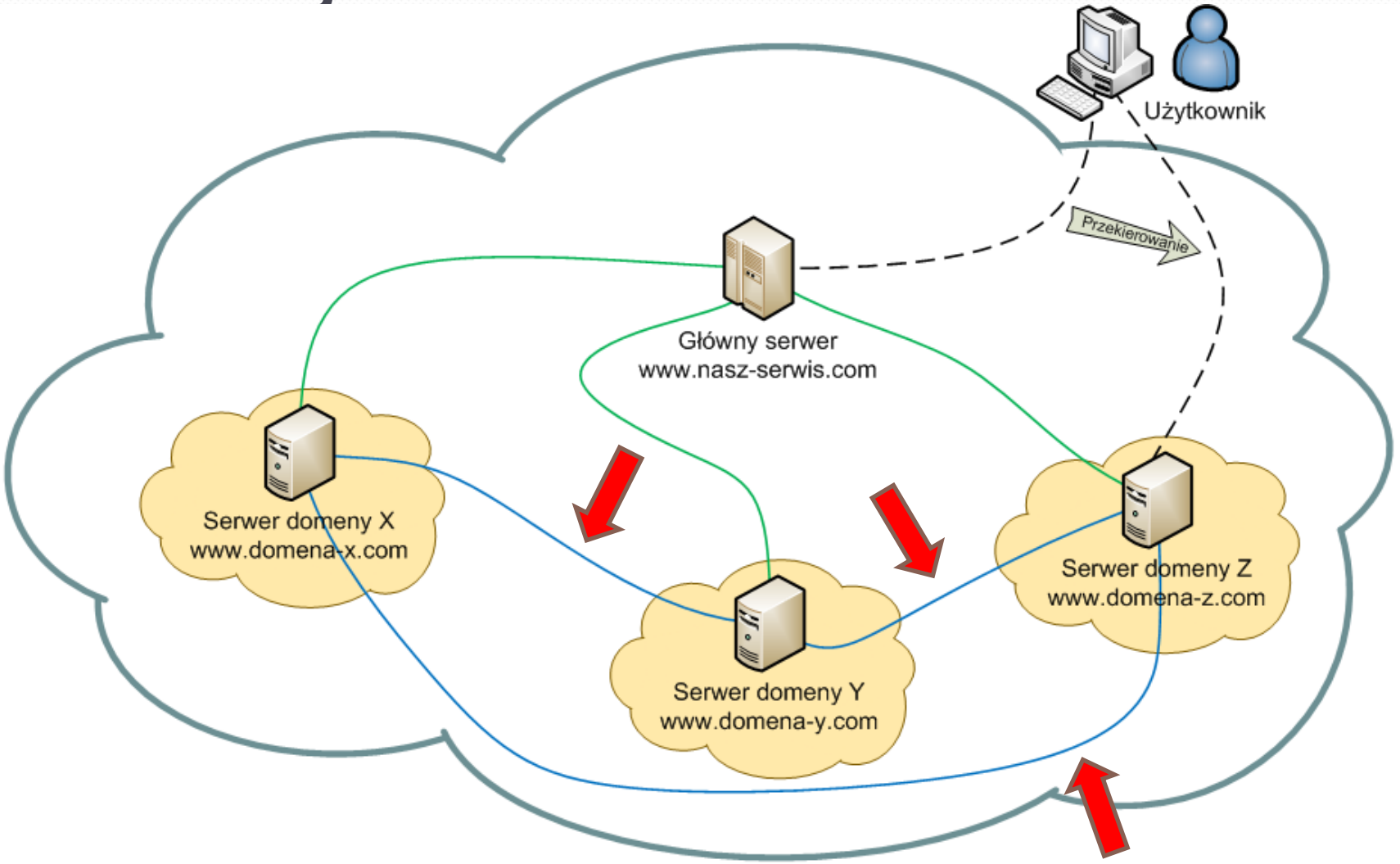
Interfejs domena-serwer



Interfejs domena-serwer

- Funkcjonalności udostępniane przez domenę:
  - Podanie udostępnianych funkcjonalności na styku
  - Podanie polityki udostępniania (co udostępniamy)
  - Podanie listy obsługiwanych użytkowników (loginy)
- Funkcjonalności udostępniane przez serwer:
  - Podanie udostępnianych funkcjonalności na styku
  - Rejestracja nowej domeny
  - Podanie obsługiwanych domen (wszystkich lub odpowiedź yes/no dla pytania o konkretną domeną)
  - Aktualizacja danych o domenie (np. adresu)

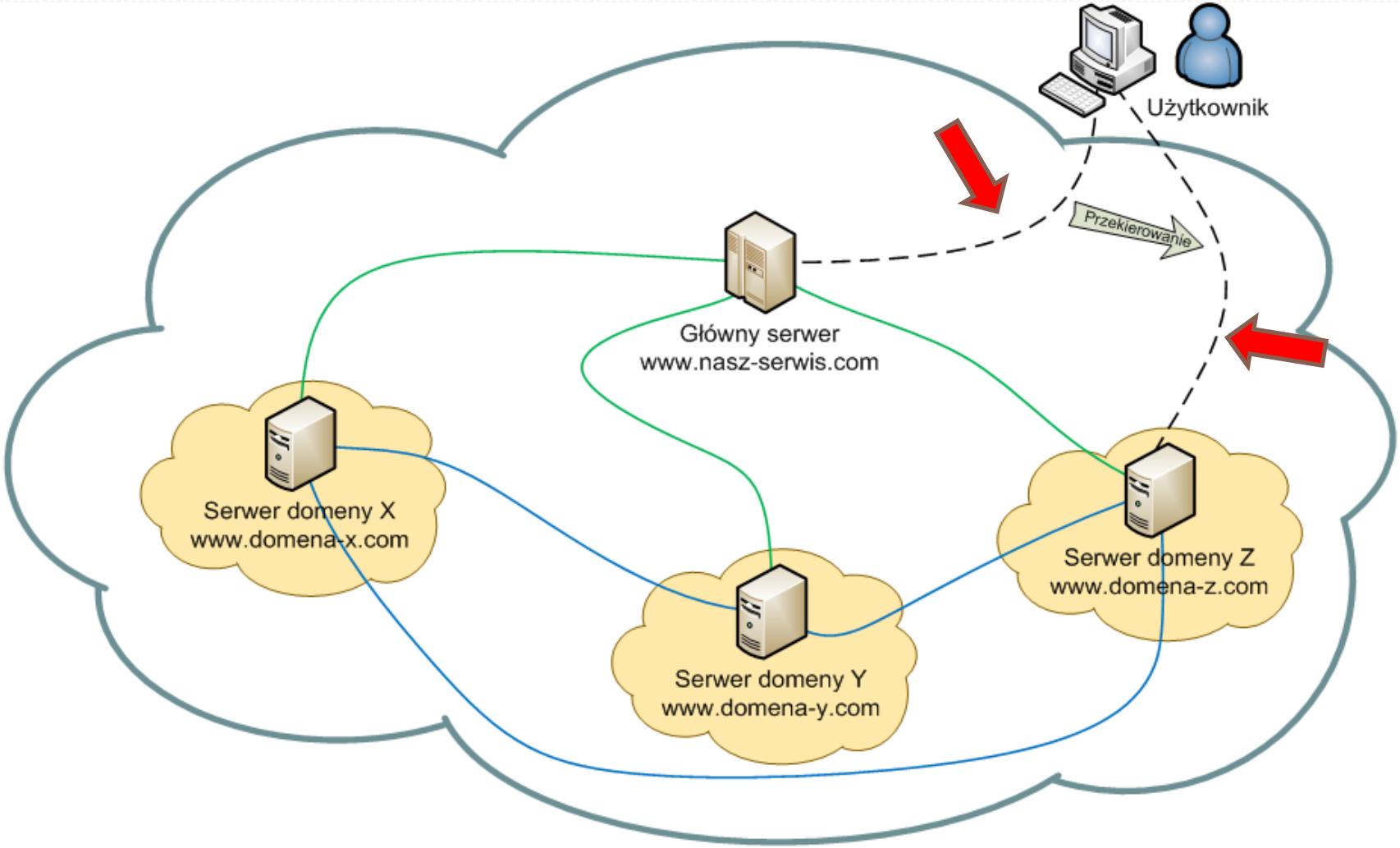
Interfejs domena-domena



Interfejs domena-domena

- Funkcjonalności udostępniane na styku domen:
  - Podanie udostępnianych funkcjonalności na tym styku
  - Podanie polityki udostępniania
  - Zwrócenie danych użytkownika (jeżeli widoczne dla innej domeny)
    - Kategoryzacja danych (np. wideo, tekst, zdjęcia)
  - Wysłanie i odpowiadanie na zapytania o dane użytkownika X
    - Mogą być zwrócone dane lub odpowiedź o braku dostępu/braku użytkownika
  - Odpowiadanie na zapytania o obecność użytkowników (online)
    - Do rozważenia model subscribe-notify (poprawi skalowalność)
  - Możliwość udostępniania dodatkowych usług (np. przez Web Services)

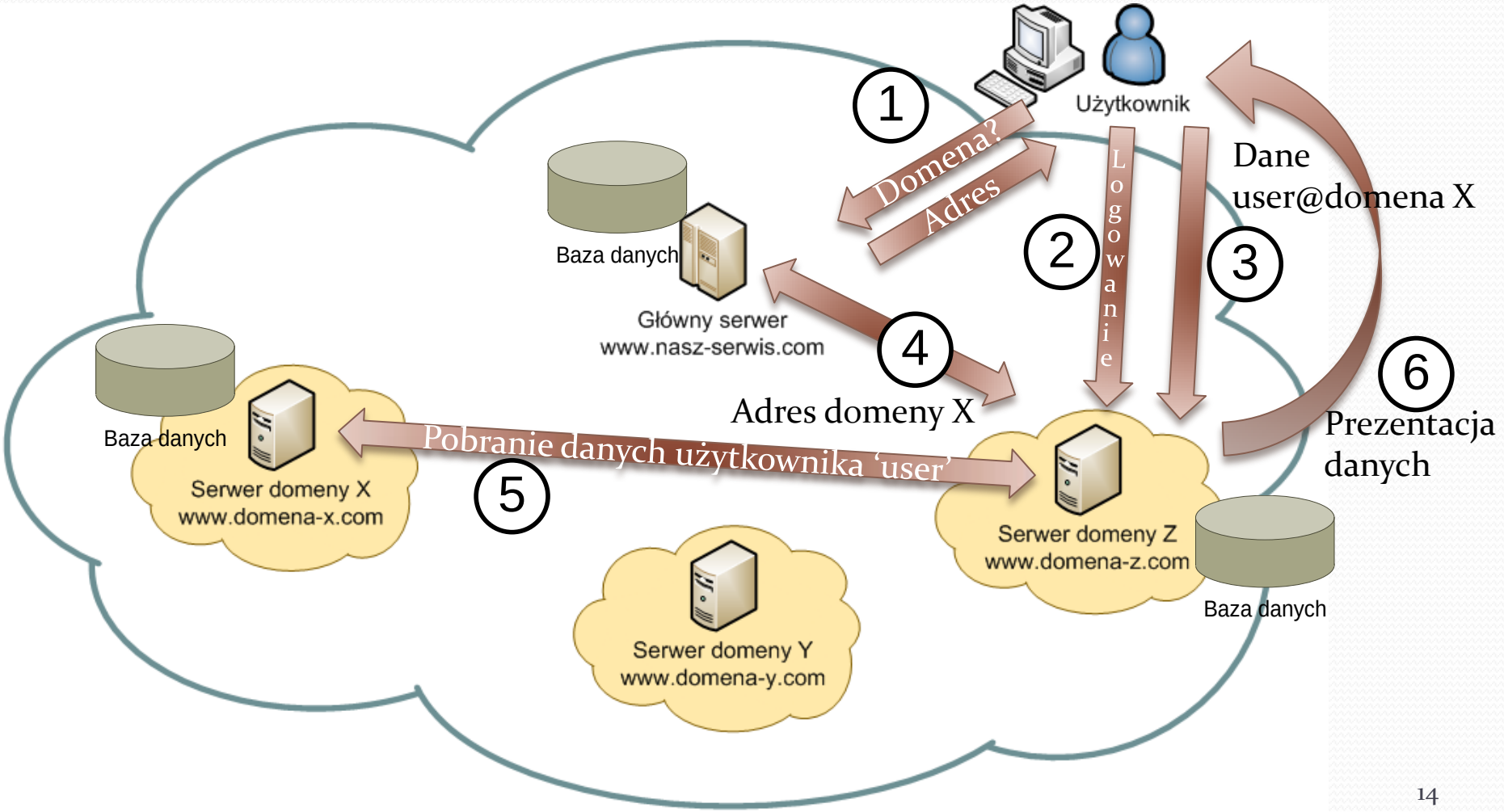
Interfejs użytkownik-serwer/domena



Interfejs użytkownik-serwer/domena

- Użytkownik może łączyć się bezpośrednio z domeną lub z serwerem głównym
- Serwer główny przekierowuje użytkownika do jego domeny
- Logowanie odbywa się zawsze w domenie
  - Serwer nie pośredniczy w logowaniu
- Użytkownik korzysta z serwisu będąc połączonym ze swoją domeną przez stronę www
- Wyniki zapytań do innych domen i do lokalnej bazy danych domeny są przetwarzane i prezentowane użytkownikowi na stronie

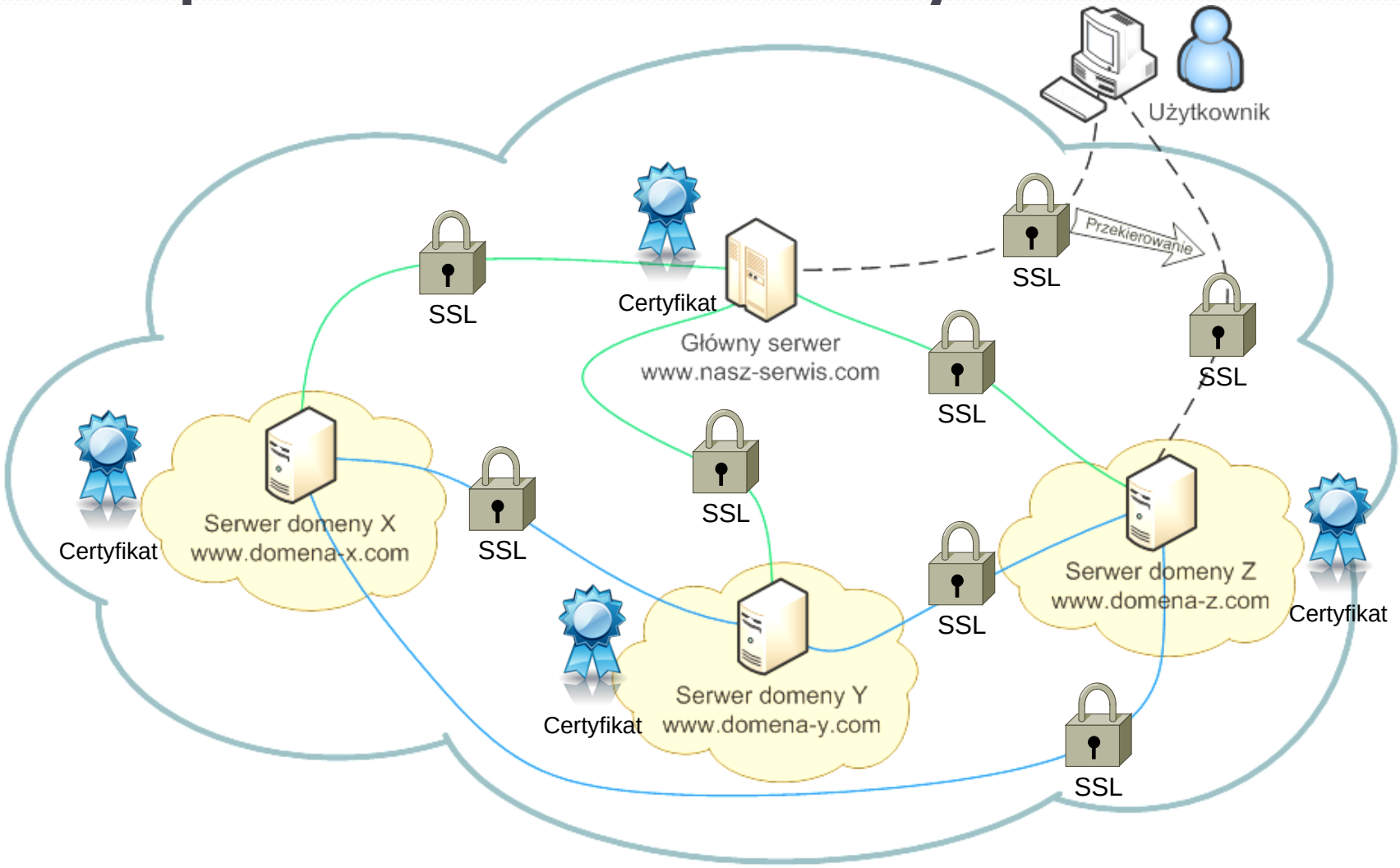
Use case – korzystanie z serwisu



Przykładowa konfiguracja domeny

- Domena uczelniana
  - Posiada adres, nazwę i opis
  - Wymiana danych tekstowych
  - Publikacja statusów i artykułów
    - Artykuły udostępniamy tylko w domenie
    - Statusy udostępniamy na zewnątrz
  - Wymiana prywatnych wiadomości
    - Udostępniane tylko określonej grupie osób
  - Użytkownik definiuje grupy udostępniania
    - Uprawnienia dla typu lub konkretnego wystąpienia zasobu
    - Udostępniamy tylko określonym użytkownikom/domenom
  - Certyfikat podpisany przez CA lub samego siebie

Bezpieczeństwo danych

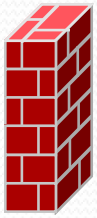


Główny serwer
www.nasz-serwis.com

Bezpieczeństwo – domena i serwer

- Szyfrowanie w bazie danych ?

- Firewall



- Wybór odpowiednich metod programistycznych

- Kontrola dostępu do kont administratorów

Bezpieczeństwo w logice serwisu

- Prosta implementacja (mniej skomplikowany kod = mniej błędów)
- Relacje ze świata rzeczywistego – kategorie osób
  - Dostępność treści dla określonych kategorii
  - Możliwość określenia domyślnych ustawień dla treści
- Weryfikacja danych użytkownika przez domenę
  - Wyświetlana informacja czy użytkownik jest zweryfikowany
- Wskaźnik reputacji (punkty nadawane przez innych użytkowników)

Zagrożenia i obrona

- Kradzież tożsamości z innego serwisu społecznościowego
  - Weryfikacja konta przez właściciela domeny
- Konta popularnych osób i dostęp do danych ich znajomych
  - Kategorie osób
- Phishing
  - Certyfikaty serwerów domenowych
  - Każda domena może mieć inną stronę logowania (ograniczenie liczby potencjalnych ofiar)

Narzędzia do wykorzystania

- Elementy AMP – Apache, MySQL, PHP
  - **Apache** – serwer HTTP
  - **MySQL** – relacyjny system baz danych
  - **PHP** – język skryptowy, umożliwia tworzenie dynamicznych witryn internetowych
  - Są to aplikacje *open source*
- Firewall (np. systemowy)
- Generator certyfikatów (np. pakiet openSSL)
- WebServices (komunikacja domena-domena i domena-serwer)

Plan działania

- Weryfikacja założeń i architektury
- Prosta implementacja
- Testy i wprowadzanie poprawek
- Weryfikacja funkcjonalności serwisu
- Wprowadzenie nowych funkcjonalności
- Testy „zewnętrzne” (większa liczba użytkowników)
- Rozpatrywanie sugestii i zgłoszonych błędów
- Poprawki w serwisie

Dziękuję za uwagę

Zachęcam do zadawania pytań i komentarzy ☺