

IBM Software

# IBM WebSphere Impact2012

The Premier Conference for Business and IT Leadership

**12-13 września 2012 r.**

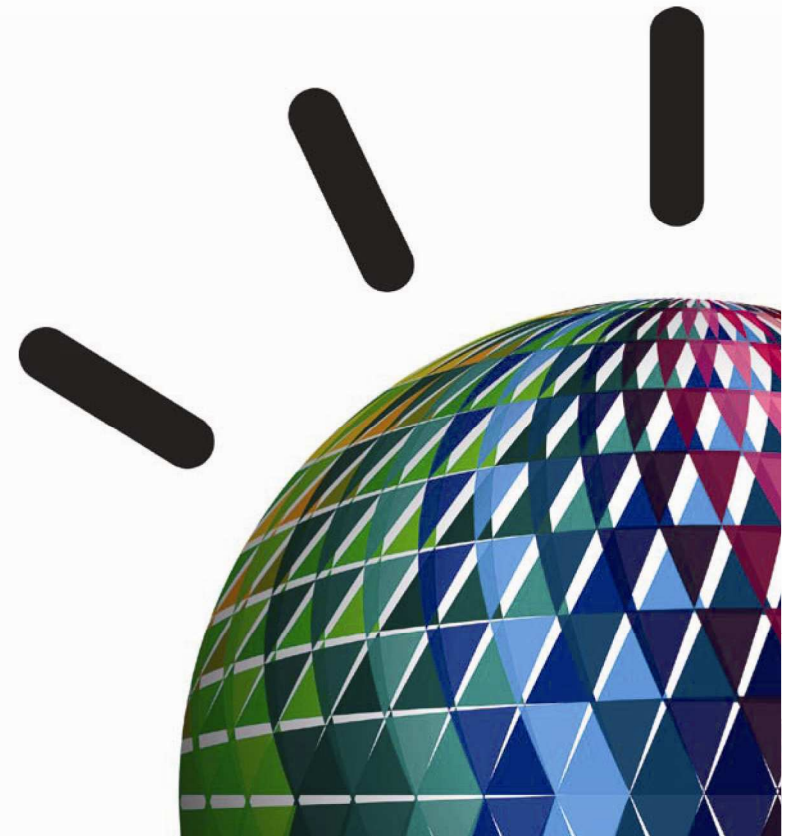
Pałac Odrowążów, Chlewiska

[www.manorhouse.pl](http://www.manorhouse.pl)

WebSphere MQ – rozwiązanie  
innowacyjne, bezpieczne i  
skuteczne w każdym biznesie.

Andrzej Kowalczyk

© 2012 IBM Corporation



# WebSphere MQ

## Do czego służy?

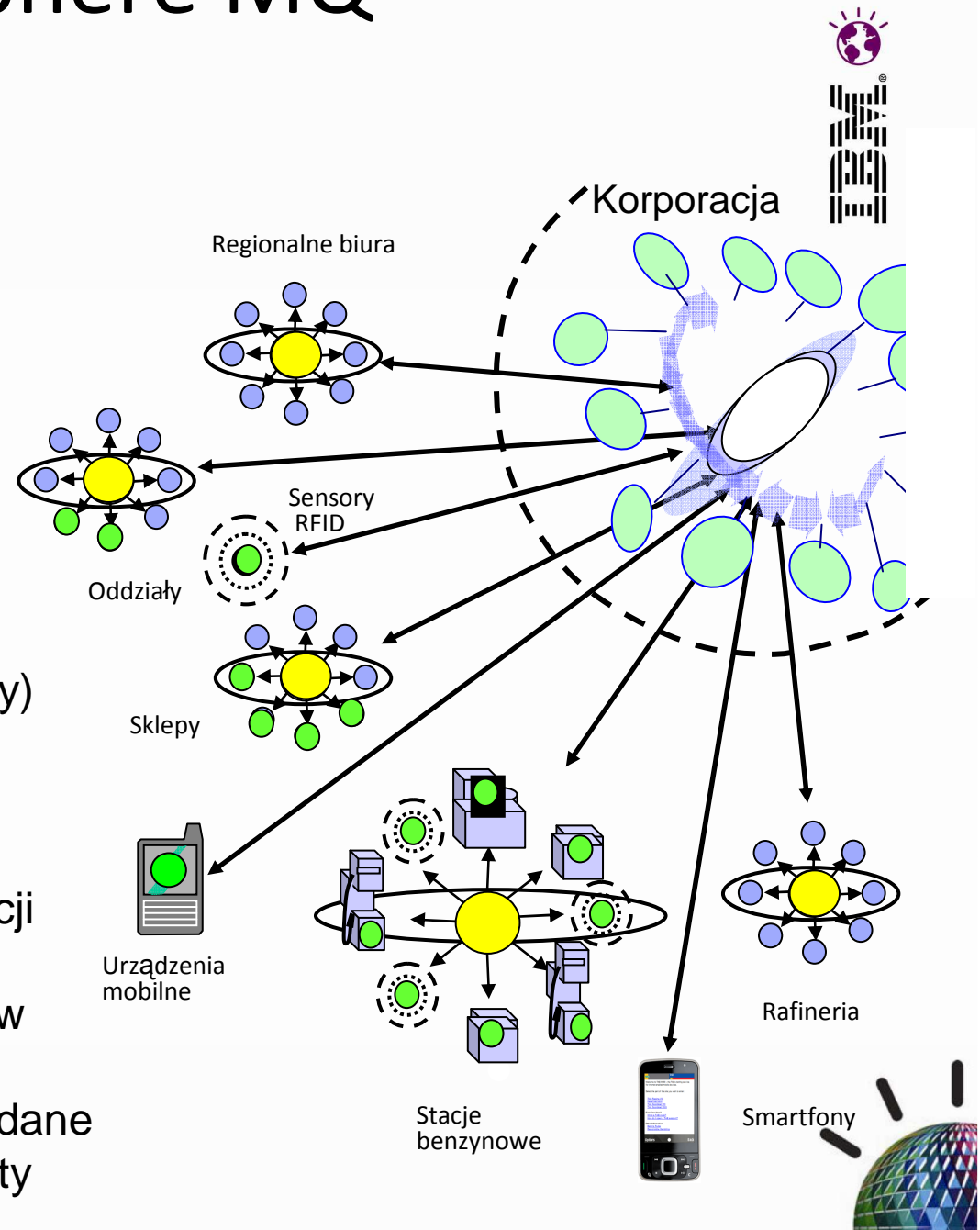
- Integracji systemów
- Wymiany informacji
- Przesyłu danych

## Kto wykorzystuje?

- Banki i sektor finansowy
- Sektor ubezpieczeniowy
- Telekomunikacja
- Energetyka & Utilities
- Sektor publiczny
- Sektor rozrywkowy (bukmacherzy)
- Sieci detaliczne

## Co zdecydowało o wyborze?

- Gwarancja dostarczenia informacji
- Szybkość
- Z dowolnego miejsca w miejsce w dowolne
- Przesyła dowolną treść: obrazy, dane tekstowe, dane finansowe, obiekty



# WebSphere MQ 7.5



- WebSphere MQ
- WebSphere MQ Multi-Instance
- WebSphere MQ AMS
- WebSphere MQ Managed File Transfer
- WebSphere MQ Telemetry



# WebSphere MQ V7.5: Główne cechy



Uproszczona architektura

Zwiększone bezpieczeństwo

Zwiększona wydajność – najszybsze WMQ w historii

Mocno „odchudzona” konsola administracyjna

Wsparcie dla wysokiej dostępności

Wsparcie dla urządzeń mobilnych





# Wiele instalacji



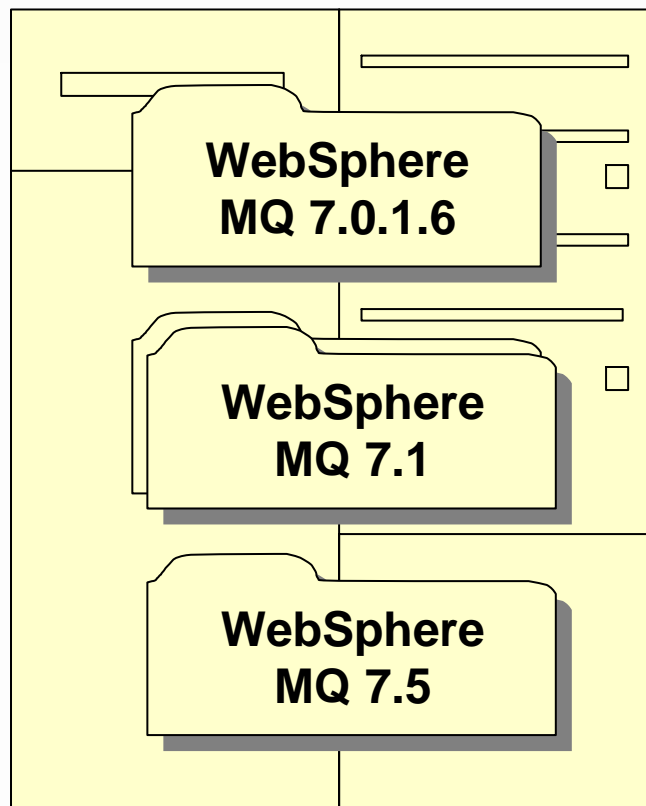
# Instalacja typu Multi-Version

WebSphere MQ 7.5



Administ

Tester



Programista



Architekt



# Instalacja typu Multi-Version



- MQ dla Unix i Windows możliwość instalacji wielo poziomowej
  - Przenaszalne do katalogu wybranego przez użytkownika
  - Może posiadać wiele kopii nawet w tej samej wersji fixpack'a
- Uproszczona migracja
  - Możliwość przenoszenia aplikacji krok po kroku, nie wszystkie za jednym razem
  - Brak konieczności posiadania dodatkowego sprzętu
- Łatwość dla ISV do używania MQ we własnych rozwiązaniach
  - Możliwość instalacji we “własnej” lokalizacji bez wpływu na inne kopie
  - Redukcja wsparcia administratorów i czynności administracyjnych
- Tylko jedna kopia V7.0.1 pozostaje w systemie
  - Możliwość „powolnej” migracji
  - wersja 7.0.1.6 lub wyższa



# Instalacja Multi-Version



- Głównym pomysłem jest **instalacja**
  - Wskazuje katalog zawierającej binaria dla konkretnej wersji MQ
  - Może posiadać nazwy opisowej
- Jedna z instalacji może być wskazana jako **podstawowa (primary)**
  - Wymagane dla Windows gdzie pewne elementy specyficzne dla systemu operacyjnego muszą być zarejestrowane
  - Optionalne dla Unix, tworzy „symlinks” do instrukcji i bibliotek w /usr
    - Nie tworzone domyślnie, PATH może nie wskazywać do właściwego katalogu
- Queue Manager’y są **własnością** konkretnej instalacji
  - Nadzór nad poziomem funkcji dostępny dla uruchomionego queue manager’a
  - Własność może być zmieniona do nowszej instalacji w celu migracji





# Przykłady z administracji



```
$ /usr/mqm/bin/dspmqrver -i
Name:      WebSphere MQ
Version:   7.1.0.0
Level:     p000-L110915
BuildType: IKAP - (Production)
Platform:  WebSphere MQ for AIX
Mode:      64-bit
O/S:       AIX 6.1
InstName:  Installation1
InstPath:  /usr/mqm
InstDesc:  My default installation
DataPath:  /var/mqm
Primary:   Yes
MaxCmdLevel: 710
```

```
Name:      WebSphere MQ
Version:   7.1.0.0
InstName:  Installation2
InstPath:  /usr/mqm2/usr/mqm
InstDesc:  A second installation
Primary:   No
```

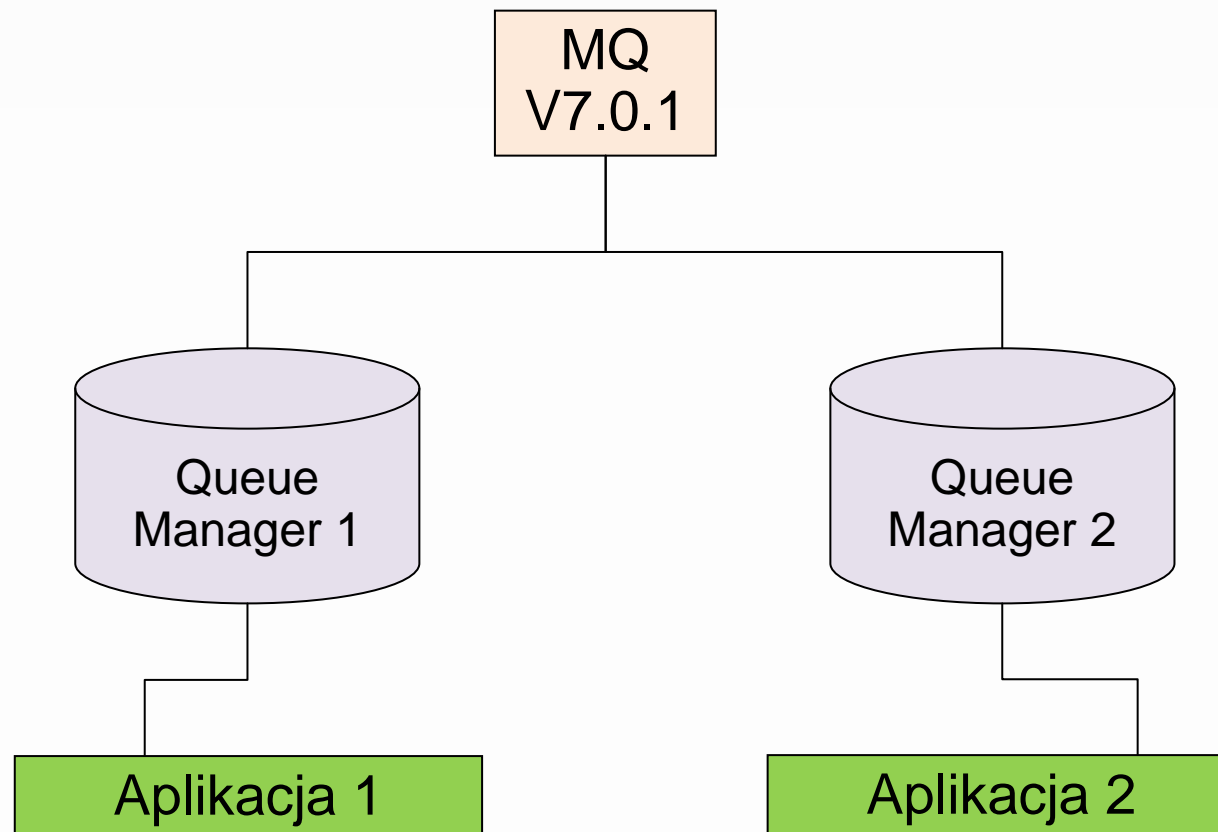
```
$ dspmq -o installation
QMNAME(V71A)
      INSTNAME(Installation1)
      INSTPATH(/usr/mqm)
      INSTVER(7.1.0.0)
QMNAME(V71B)
      INSTNAME(Installation1)
      INSTPATH(/usr/mqm)
      INSTVER(7.1.0.0)
QMNAME(INST2QM)
      INSTNAME(Installation2)
      INSTPATH(/usr/mqm2/usr/mqm)
      INSTVER(7.1.0.0)
```

```
$ /usr/mqm/bin/endmqm INST2QM
AMQ5691: Queue manager 'INST2QM'
is associated with a different installation.
```



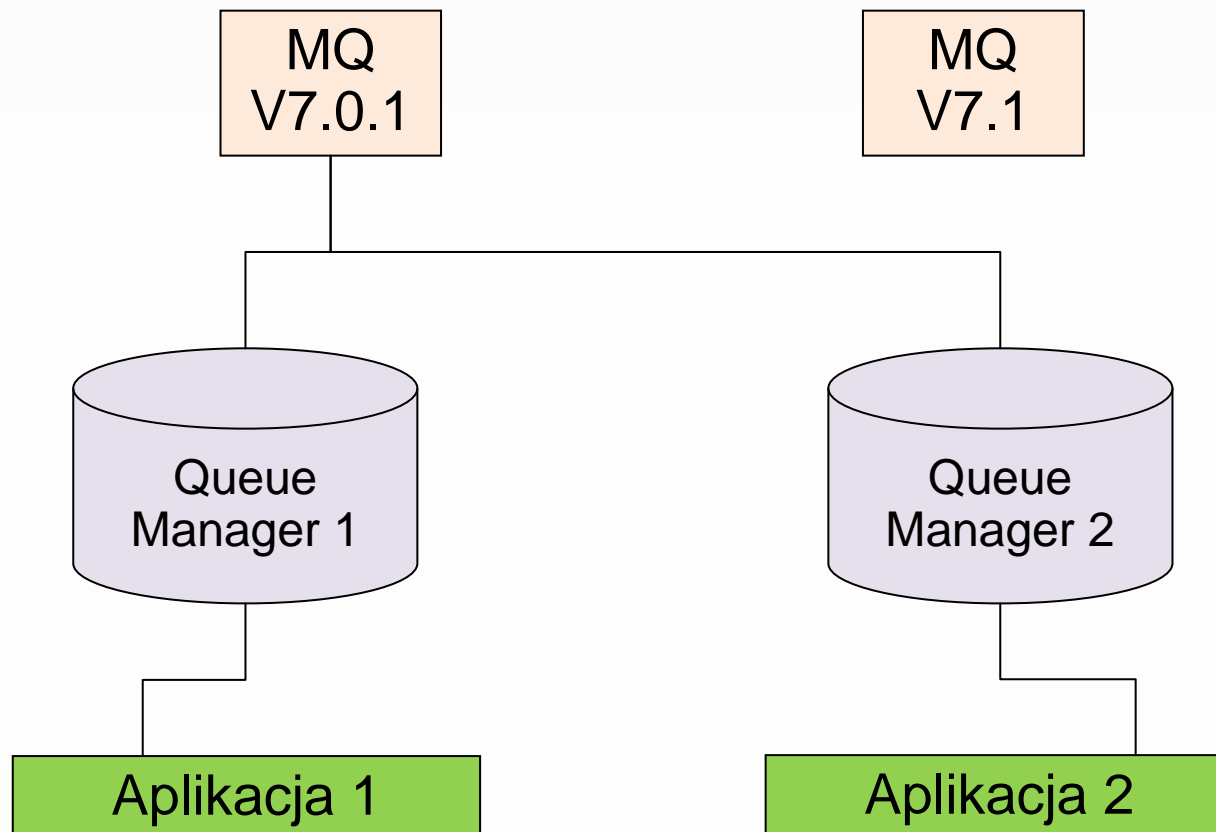
# Migracja aplikacji: (1) Identyfikacja

## Aplikacji do migracji

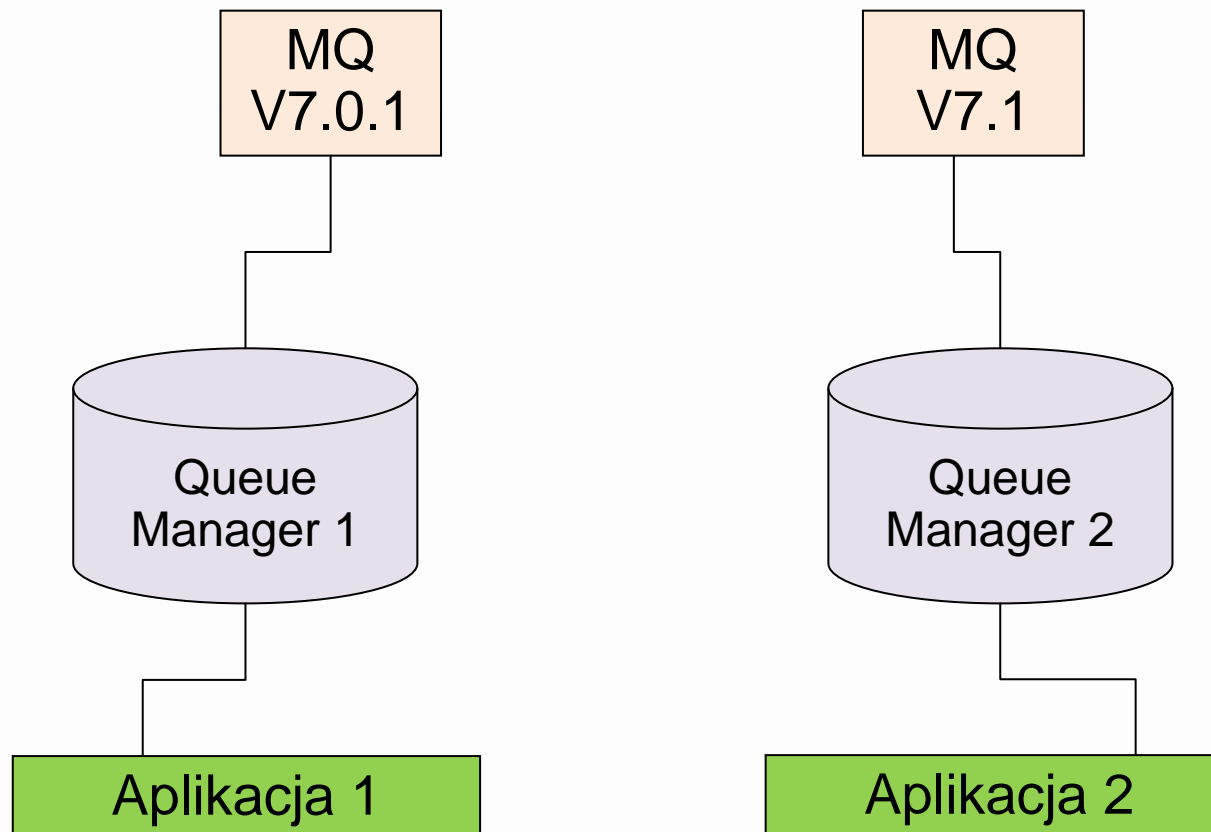


# Migracja aplikacji:(2) Instalacja

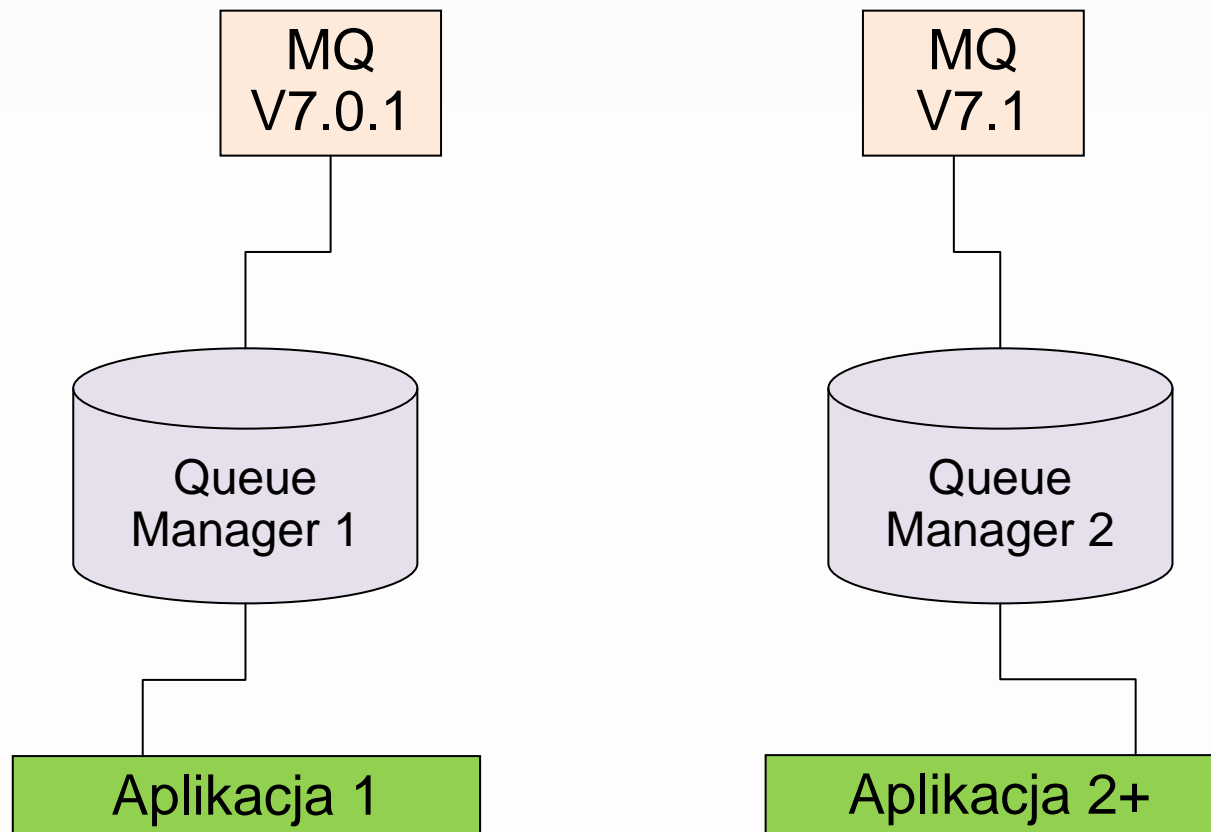
## V7.1 obok V7.0.1



# Migracja aplikacji:(3) skojarzenie kodu V7.1 z QMgr



# Migracja aplikacji:(4) Zmiana aplikacji



# Zalety Multi-Version



- Prostsza migracja do nowych wersji
- Łatwiejsza instalacja
- Współistnienie wielu wersji





# Bezpieczeństwo



# Wyzwania

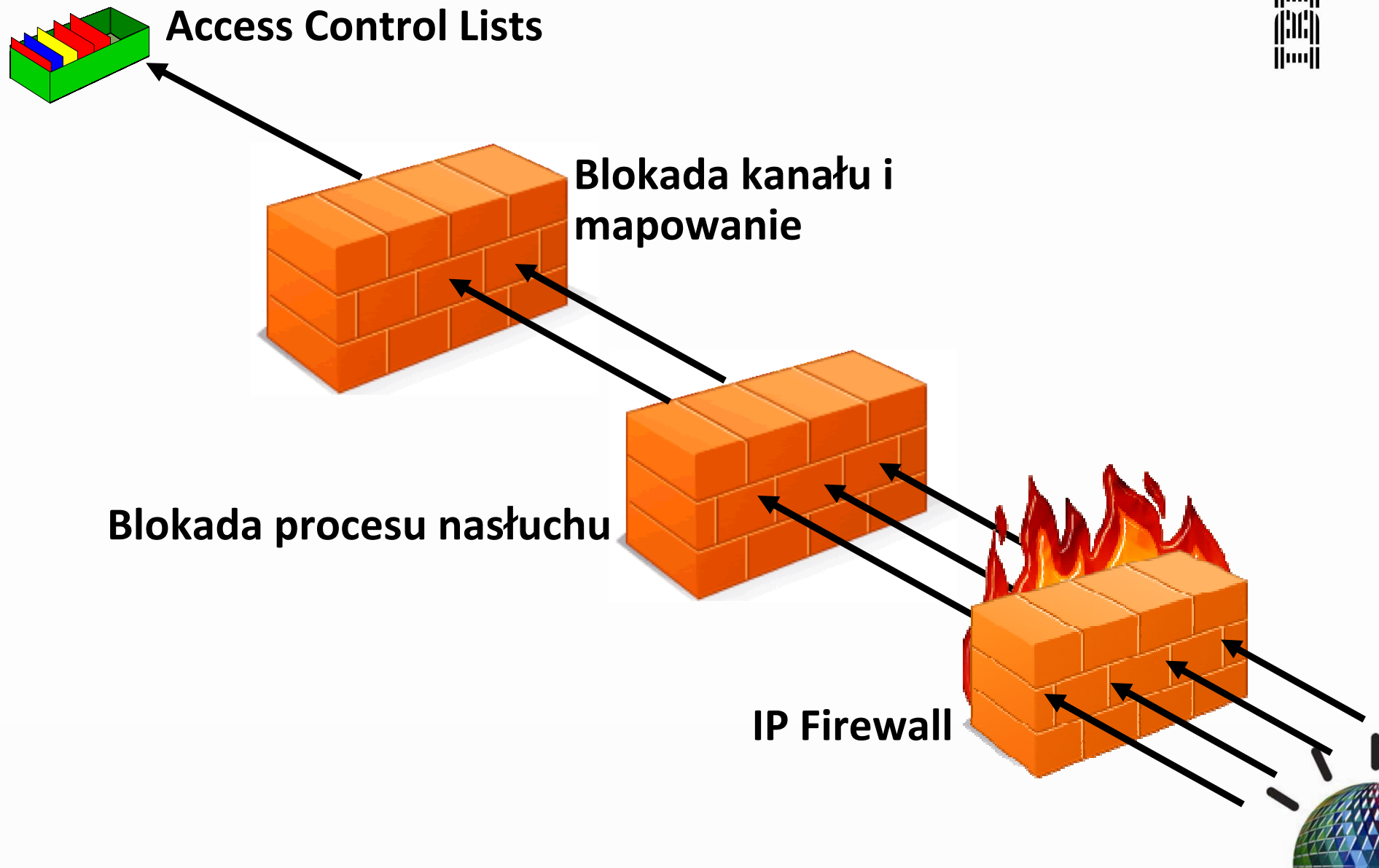


- Jak rozpoznać różnych klientów na kanałach?
- Kto wykorzystuje moje kanały i jakie ma uprawnienia?
- Czy muszę tworzyć kanał dla każdego klienta zewnętrznego?





# Bezpieczeństwo dostępu do kanału



# Scenariusz dostępu do kanału (1)



```
SET CHLAUTH(*) TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
```



“Musimy mieć pewność, że nasz system jest całkowicie bezpieczny”



# Scenariusz dostępu do kanału (2)



```
SET CHLAUTH(*) TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
```

```
SET CHLAUTH(BPCHL.*) TYPE(SSLPEERMAP) SSLPEER('O=Bank of Shetland')  
MCAUSER(BANK123)
```

```
SET CHLAUTH(BPCHL.*) TYPE(SSLPEERMAP) SSLPEER('O=Bank of Orkney')  
MCAUSER(BANK456)
```



“Nasi Partnerzy biznesowi muszą wszystkie połączenia realizować za pomocą SSL, a do ich identyfikacji będziemy wykorzystywać certyfikat cyfrowy.



# Scenariusz dostępu do kanału (3)



```
SET CHLAUTH(*) TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
```

```
SET CHLAUTH(BPCHL.*) TYPE(SSLPEERMAP) SSLPEER('O=Bank of Shetland')  
MCAUSER(BANK123)
```

```
SET CHLAUTH(BPCHL.*) TYPE(SSLPEERMAP) SSLPEER('O=Bank of Orkney')  
MCAUSER(BANK456)
```

```
SET CHLAUTH(SYSTEM.ADMIN.SVRCONN) TYPE(ADDRESSMAP)  
ADDRESS('9.20.1-30.*') MCAUSER(ADMUSER)
```



“Nasi administratorzy łączyć się będą za pomocą graficznej konsoli administracyjnej, ale bez SSL.

Z uwagi na to, że znamy adresy IP komputerów osobistych administratorów, dla nich ustawimy dostęp.



# Scenariusz dostępu do kanału (4)



```
SET CHLAUTH(*) TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)

SET CHLAUTH(BPCHL.*) TYPE(SSLPEERMAP) SSLPEER('O=Bank of Shetland')
MCAUSER(BANK123)

SET CHLAUTH(BPCHL.*) TYPE(SSLPEERMAP) SSLPEER('O=Bank of Orkney')
MCAUSER(BANK456)

SET CHLAUTH(SYSTEM.ADMIN.SVRCONN) TYPE(ADDRESSMAP)
ADDRESS('9.20.1-30.*') MCAUSER(ADMUSER)

SET CHLAUTH(TO.CLUS.*) TYPE(QMGRMAP)
QMNAME(CLUSQM*) MCAUSER(CLUSUSR) ADDRESS('9.30.*')
```



“Nasz wewnętrzny klaster nie używa protokołu SSL, musimy zapewnić, że tylko odpowiednie menedżery kolejek mogą połączyć się w klaster.”





Zwiększona  
wydajność mechanizmu  
publish/subscribe



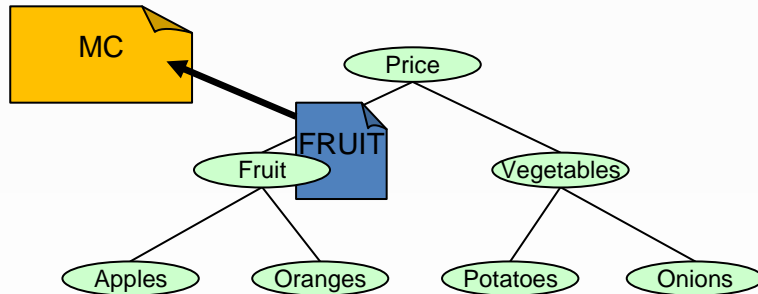
# WMQ Client – Multicast



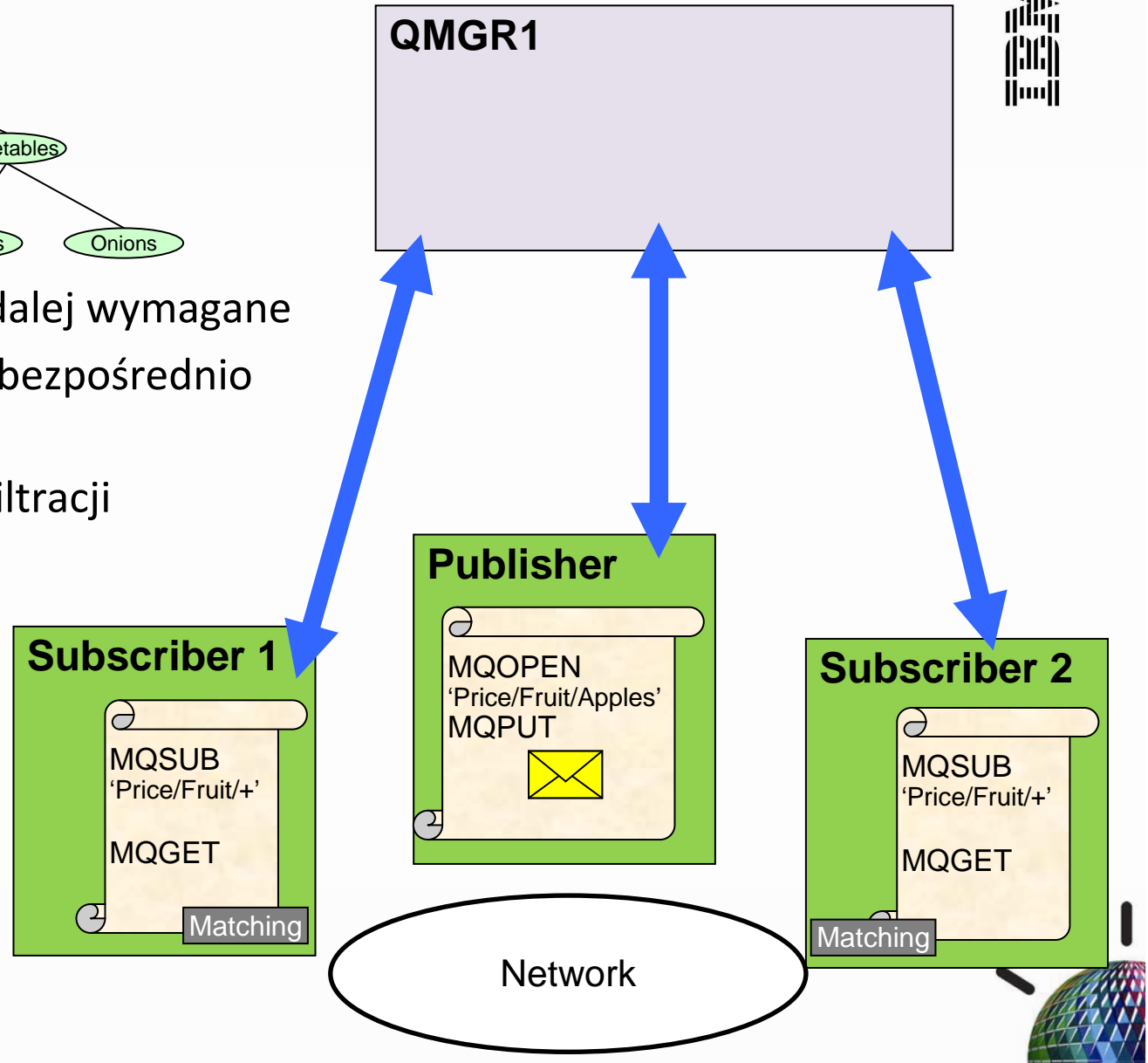
- Publish/Subscribe został rozbudowany do komunikacji typu multicast
  - Użyte technologie z produktu MQ Low Latency Messaging
- Dostarcza nowy poziom jakości
  - Bardzo duża szybkość dostarczenia komunikatów nietrwałych
  - Wyższa “uczciwość” gdyż wszyscy odbiorcy otrzymują komunikat w tym samym czasie
  - Wyższa skalowalność gdyż dodatkowi subskrybenci nie powodują dodatkowego ruchu
- Dostarcza bezpośrednie połączenie pomiędzy wydawcą a subskrybentem omijając qmgr
- Manager kolejek utrzymuje status i statystyki dla monitoringu



# Multicast Publish/Subscribe

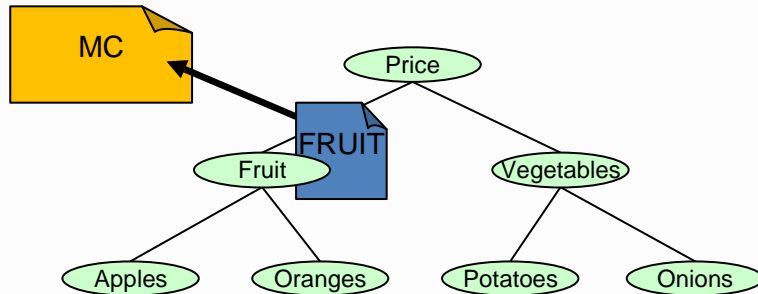


- Zwykłe połączenie MQ dalej wymagane
- Komunikaty przesyłane bezpośrednio pomiędzy klientami
- Subskrybent dokonuje filtracji

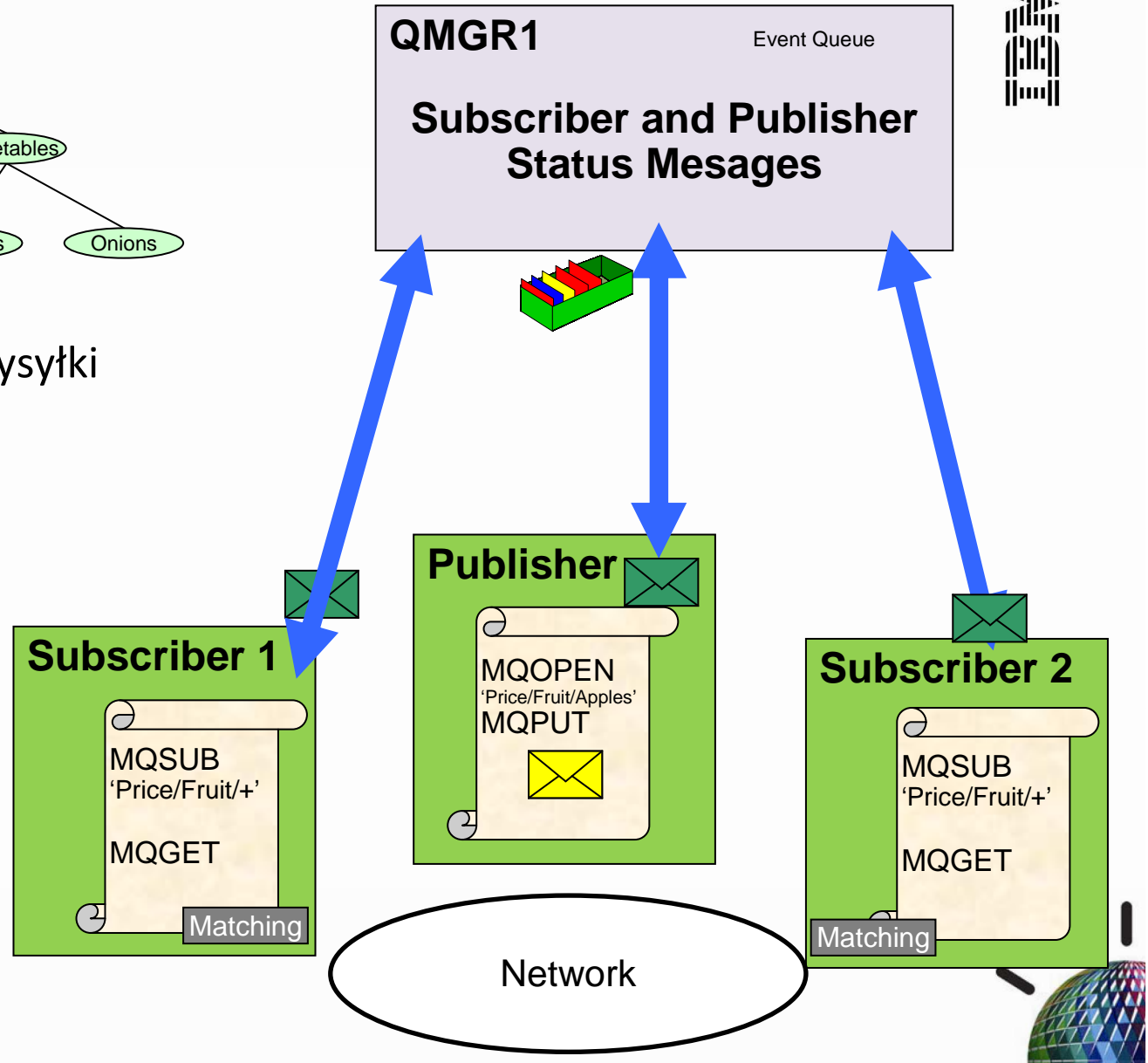




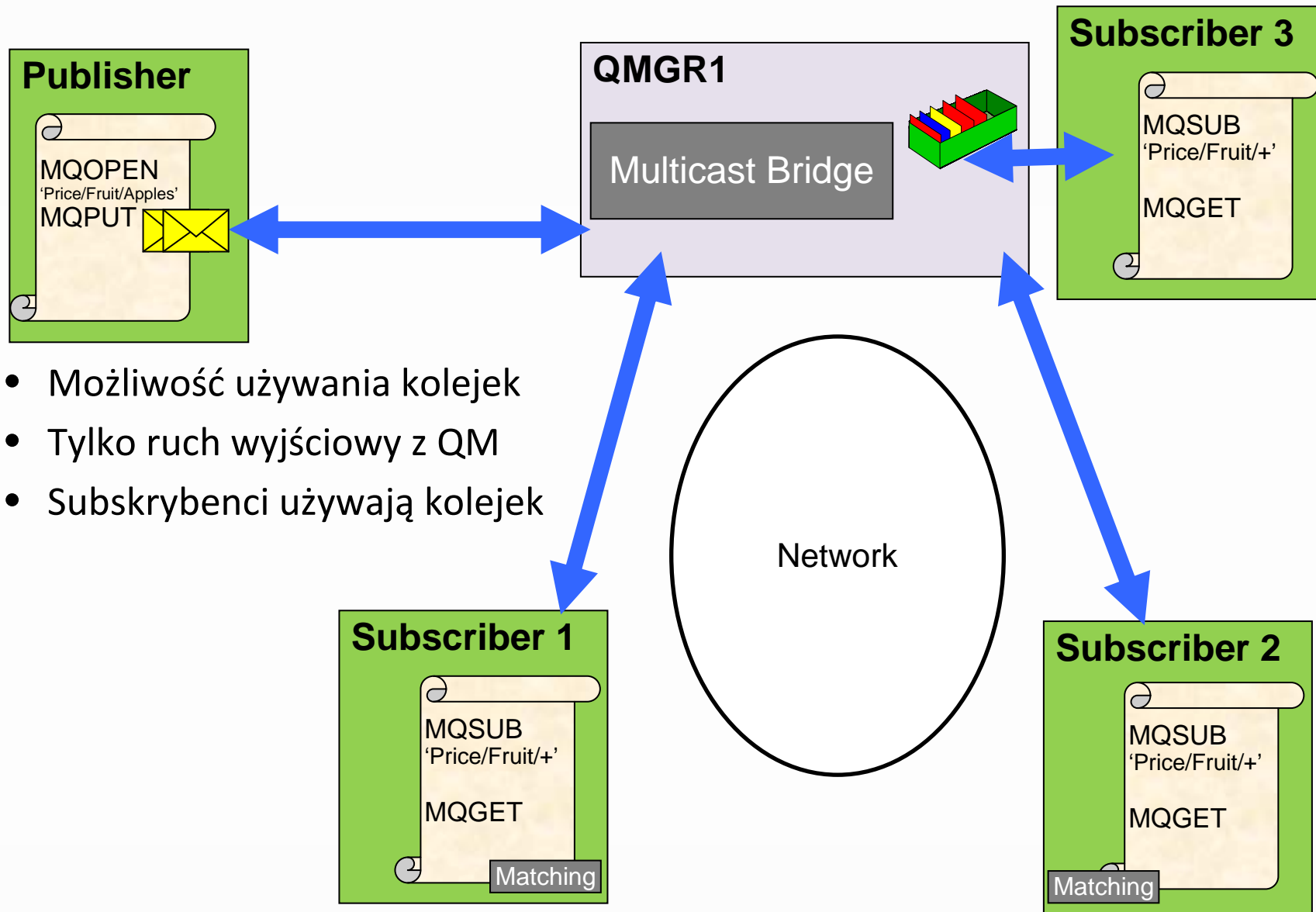
# Multicast Monitoring



- Definiowany interwał wysyłki
- Monitorowanie zmian



# Multicast Bridging & Queueing



- Możliwość używania kolejek
- Tylko ruch wyjściowy z QM
- Subskrybenci używają kolejek





# WebSphere MQ MultiInstance



# Wysoka dostępność



W jaki sposób zapewnić ciągłość działania WebSphere MQ?

Co zrobić aby nie utracić ani jednego komunikatu podczas przełączenia na zapasowy serwer?

Czy potrzeba dodatkowego oprogramowania systemowego?

Co w przypadku zmiany platformy systemowej?

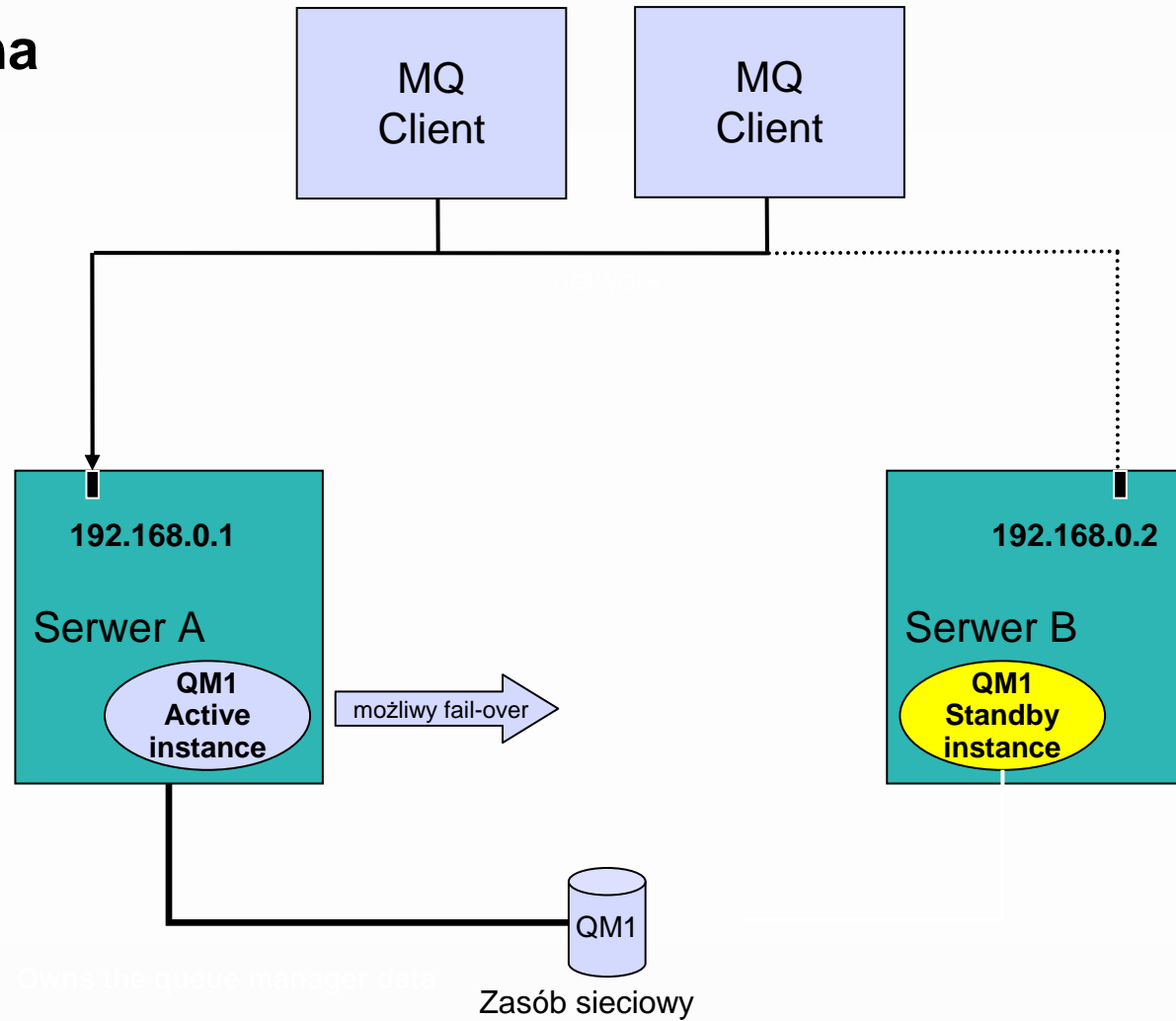
Czy WMQ przełączy się automatycznie?



# Multi-Instance



## 1. Normalna praca



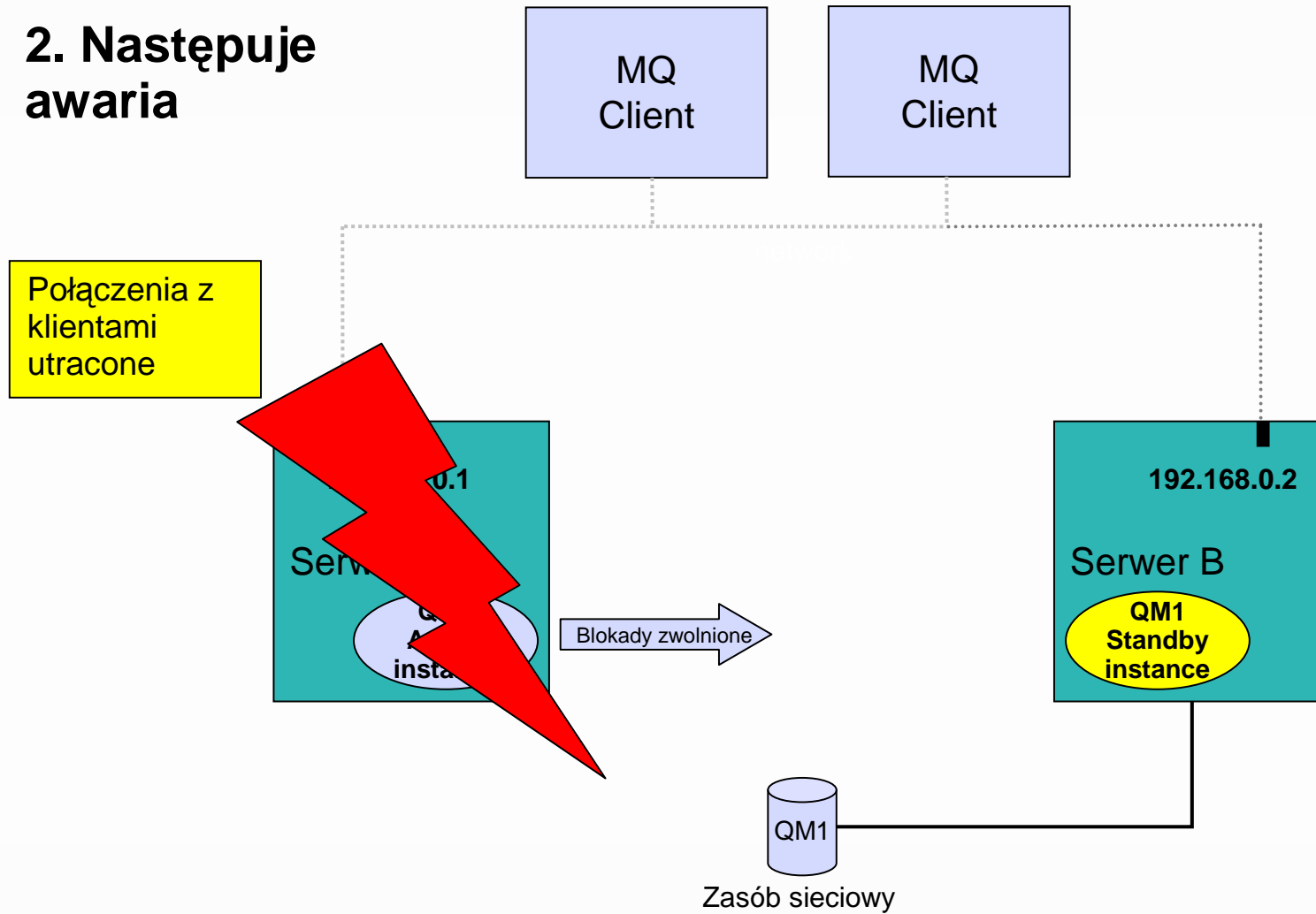
Owns the queue manager data



# Multi-Instance



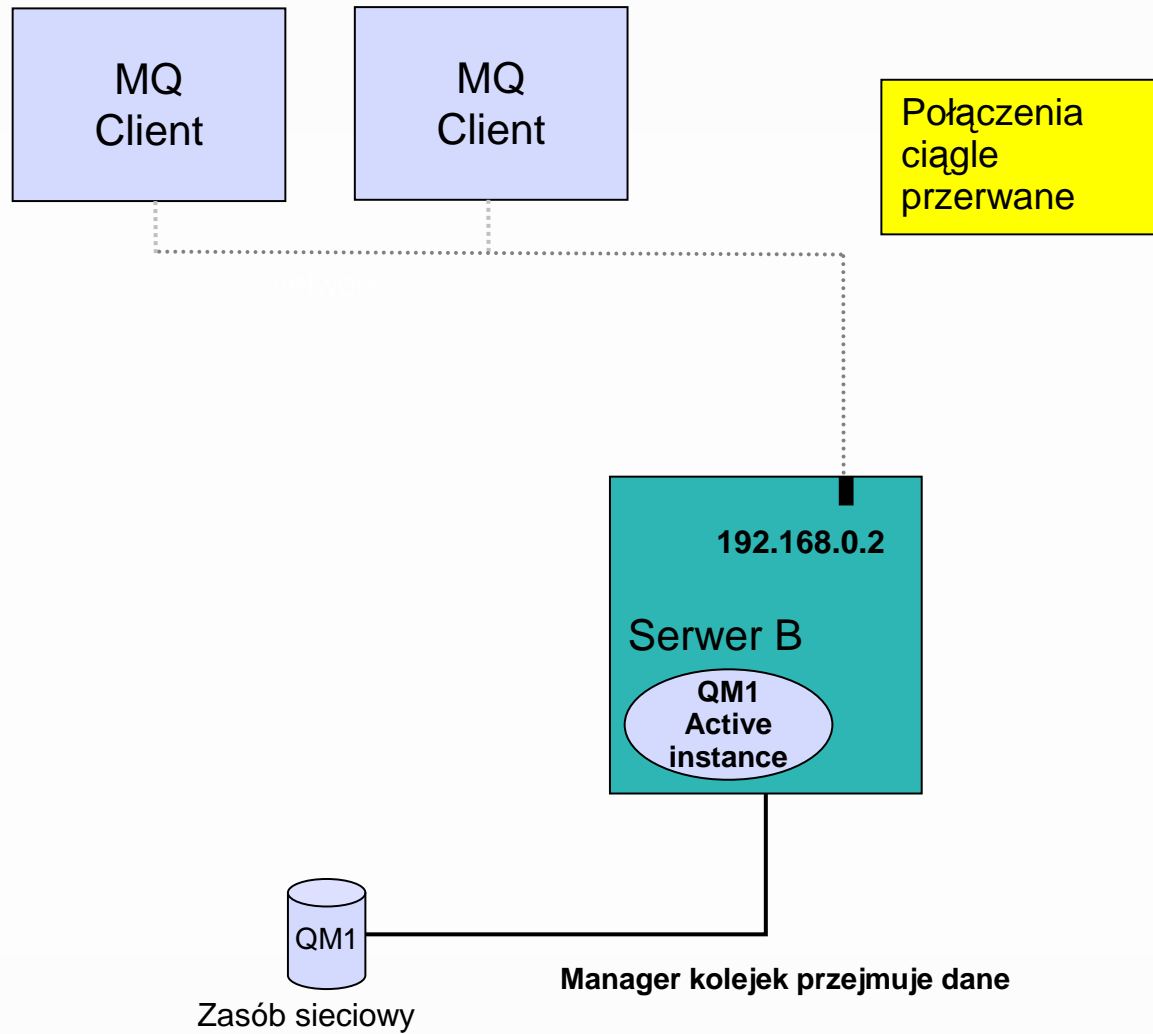
## 2. Następuje awaria



# Multi-Instance



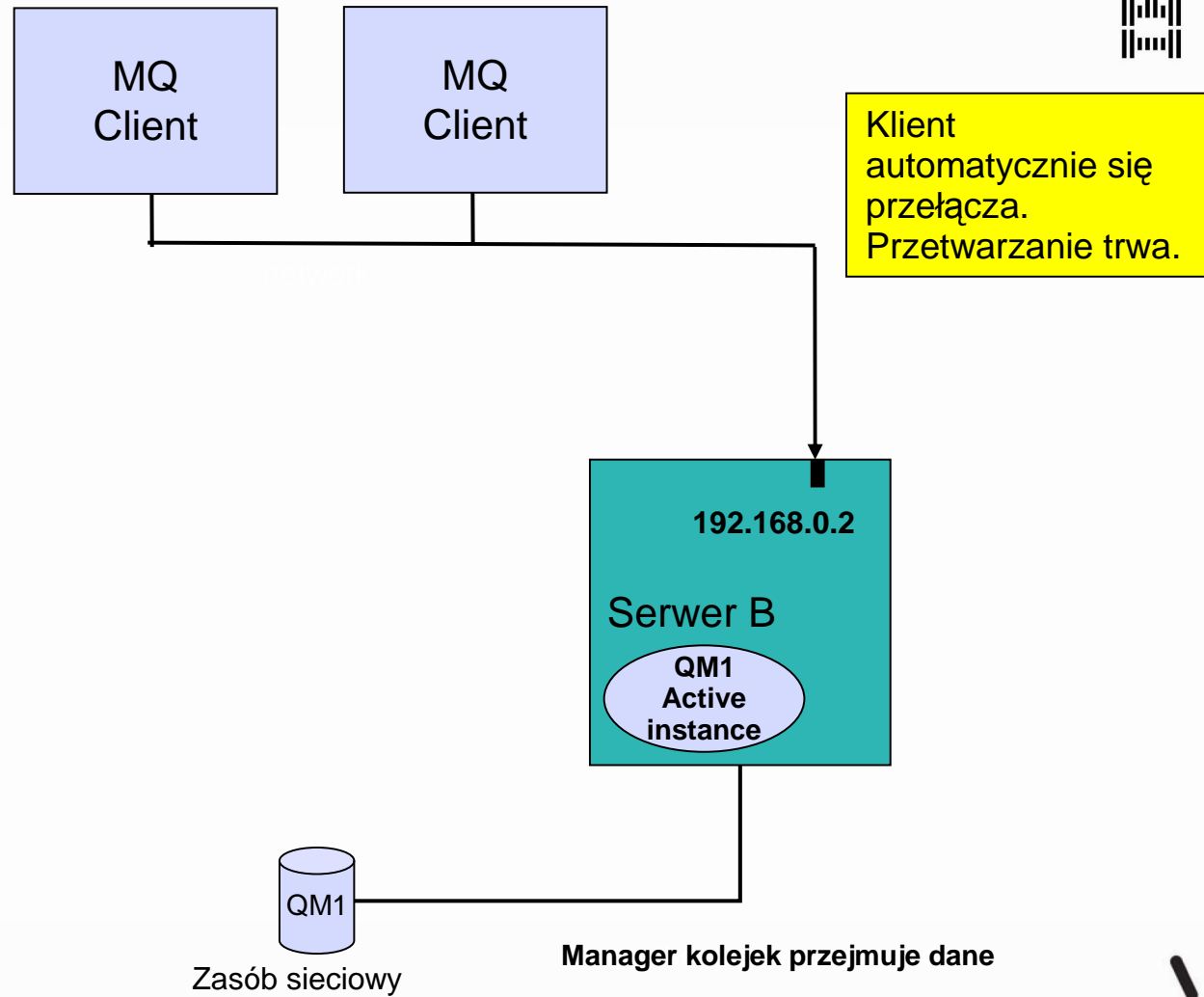
**3. QM zapasowy rozpoczyna proces przejmowania zasobów**



# Multi-Instance



## 4. Przywracanie ciągłości działania zakończone





# Multi-Instance – jak rozróżnić?



- Dodatkowe widoki dla - dspmq
- Nowe opcje dla dspmq
- W celu tworzenia skryptów

```
$ hostname  
rockall  
$ dspmq -x  
QMNAME(V7)          STATUS(Running)  
    INSTANCE(rockall)  MODE(Active)  
QMNAME(V7B)         STATUS(Running)  
    INSTANCE(rockall)  MODE(Active)  
QMNAME(V7C)         STATUS(Running as standby)  
    INSTANCE(llareggub) MODE(Active)  
    INSTANCE(rockall)  MODE(Standby)
```



# Multi-Instance – jak rozróżnić?



WebSphere MQ Explorer - com.ibm.mq.explorer.ms0p.updateSite/todo.txt - Eclipse SDK

File Edit Navigate Search Project Run Window Help

WebSphere MQ Explorer - Navigator WebSphere MQ Explorer - Content Events and Statistics

IBM WebSphere MQ

- Queue Managers
- Queue Manager Clusters
- JMS Administered Objects
- Managed File Transfer
- Service Definition Repositories
- Administered Servers
  - audi (audi.hursley.ibm.com)
  - dummy
  - rockall (rockall.hursley.ibm.com)
- Thin Clients
- Brokers
- Broker Resources
- MQSC Scripts

### Queue Managers on rockall

| Name    | Listener Port | QMID                   | Admin Obje... | State              | Instances                           |
|---------|---------------|------------------------|---------------|--------------------|-------------------------------------|
| ATS_AIX | 3414          | ATS_AIX_2009-04-21...  | No            | Running            | rockall(Active)                     |
| linear  | 1414          | linear_2009-04-21_1... | Yes           | Running            | rockall(Active)                     |
| V53     | Unknown       | Unknown                | Unknown       | Stopped            | Unknown                             |
| V7      | 2414          | V7_2009-04-21_12.3...  | Yes           | Running            | rockall(Active)                     |
| V7B     | 2415          | V7B_2009-04-21_12....  | Yes           | Running            | rockall(Active)                     |
| V7C     | Unknown       | Unknown                | Unknown       | Running as standby | llareggub(Active), rockall(Standby) |

| Source | Destination | Current File | File Number | Progress | Rate | Started (Europe/London) |
|--------|-------------|--------------|-------------|----------|------|-------------------------|
|--------|-------------|--------------|-------------|----------|------|-------------------------|



# Multi-Instance



Mechanizm wysokiej dostępności dostępny „z pudełka”

Nie wymaga dodatkowego oprogramowania czy sprzętu

Prosta konfiguracja

Automatyczne przełączanie bez utraty komunikatów  
(trwałych)

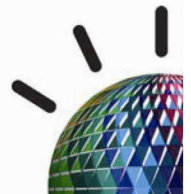
Niski koszt całego rozwiązania

Identyczny mechanizm dla produktów wykorzystujących  
WMQ – WebSphere Message Broker czy WMQ MFT

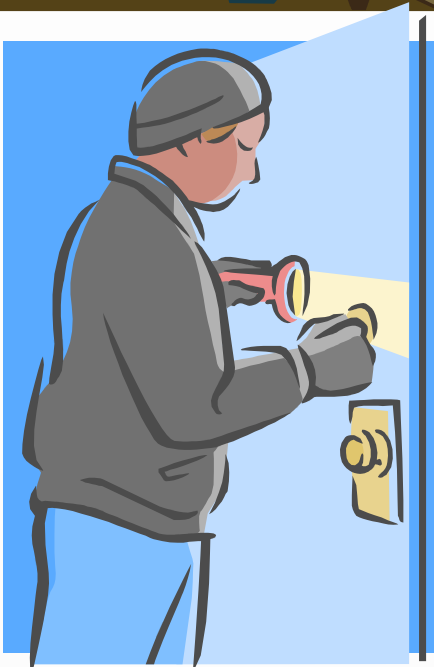




# WebSphere MQ AMS



# Jakie bezpieczeństwo jest tym właściwym?



# Jak rozpoznać zagrożenie?





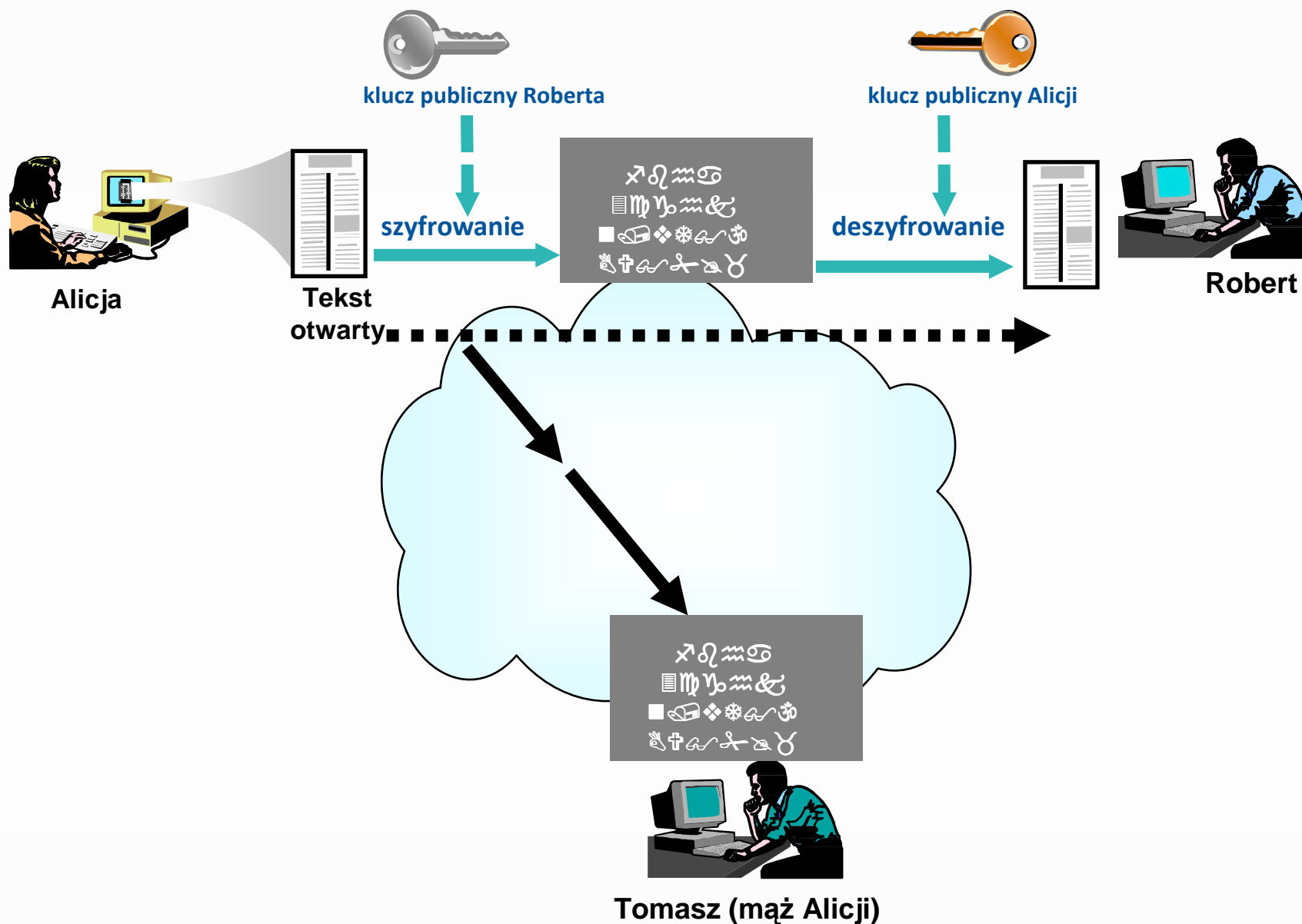
# Bezpieczeństwo komunikatu



- Komunikacja WMQ nie zawsze angażuje ludzi
  - Aplikacja → Aplikacja
  - Oczekiwanie przetwarzanie w czasie rzeczywistym lub zbliżonym do niego
  - Bezpieczeństwo coraz bardziej wymagane ze względu na brak „ludzkiego nadzoru”
- Nie wszystkie komunikaty są identyczne
  - Różne scenariusze
  - Komunikaty kontrolne
  - Zawierają dane podlegające audytowi
- Dane i standardy kontroli
  - Dane z kart kredytowych - spełnienie PCI
  - Poufne dane rządowe
  - Dane osobowe

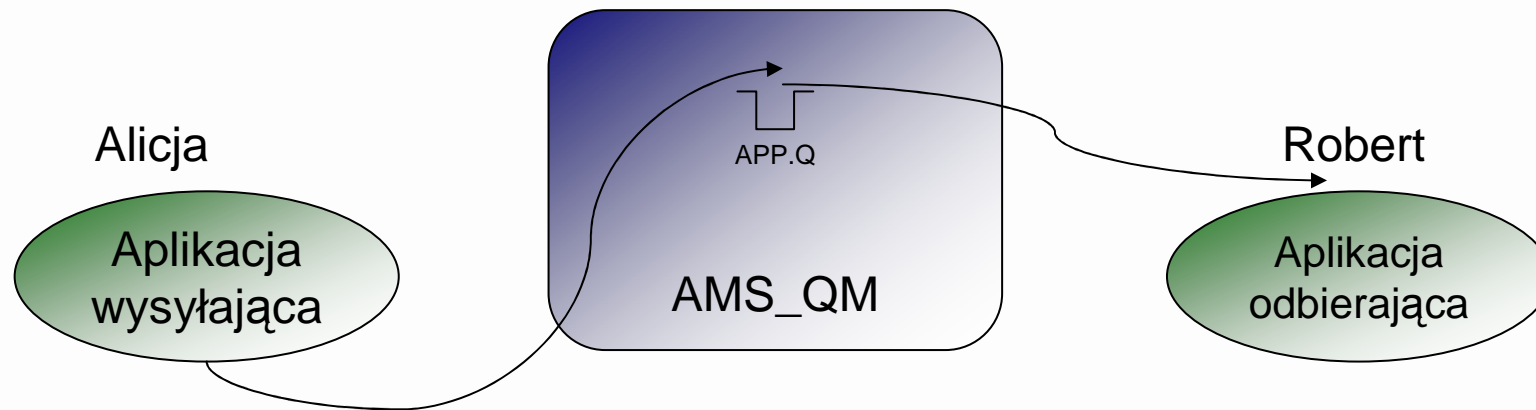


# Zazdrosny mąż

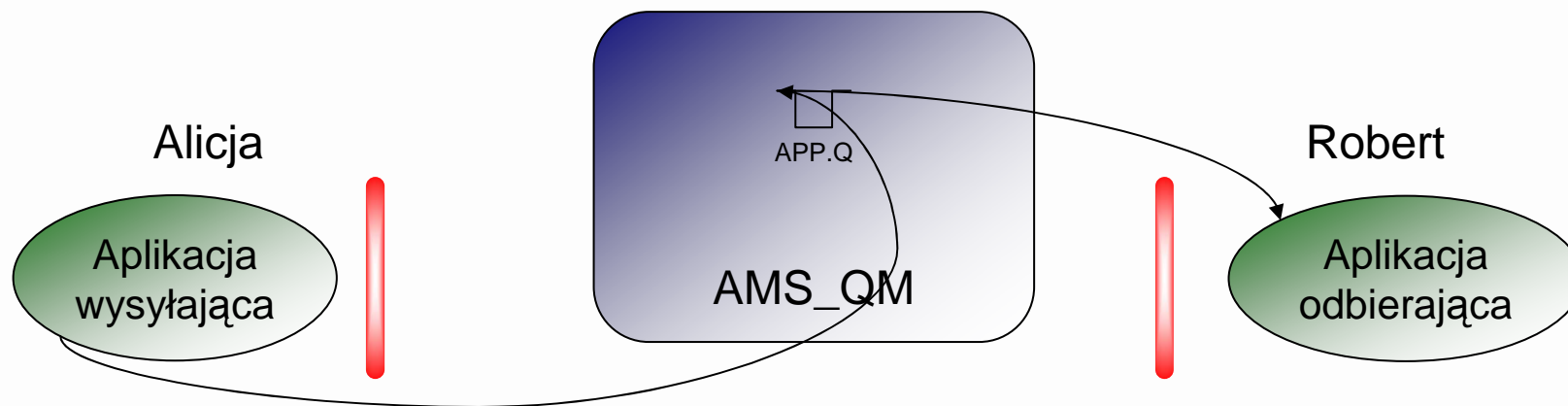




# WebSphere MQ AMS



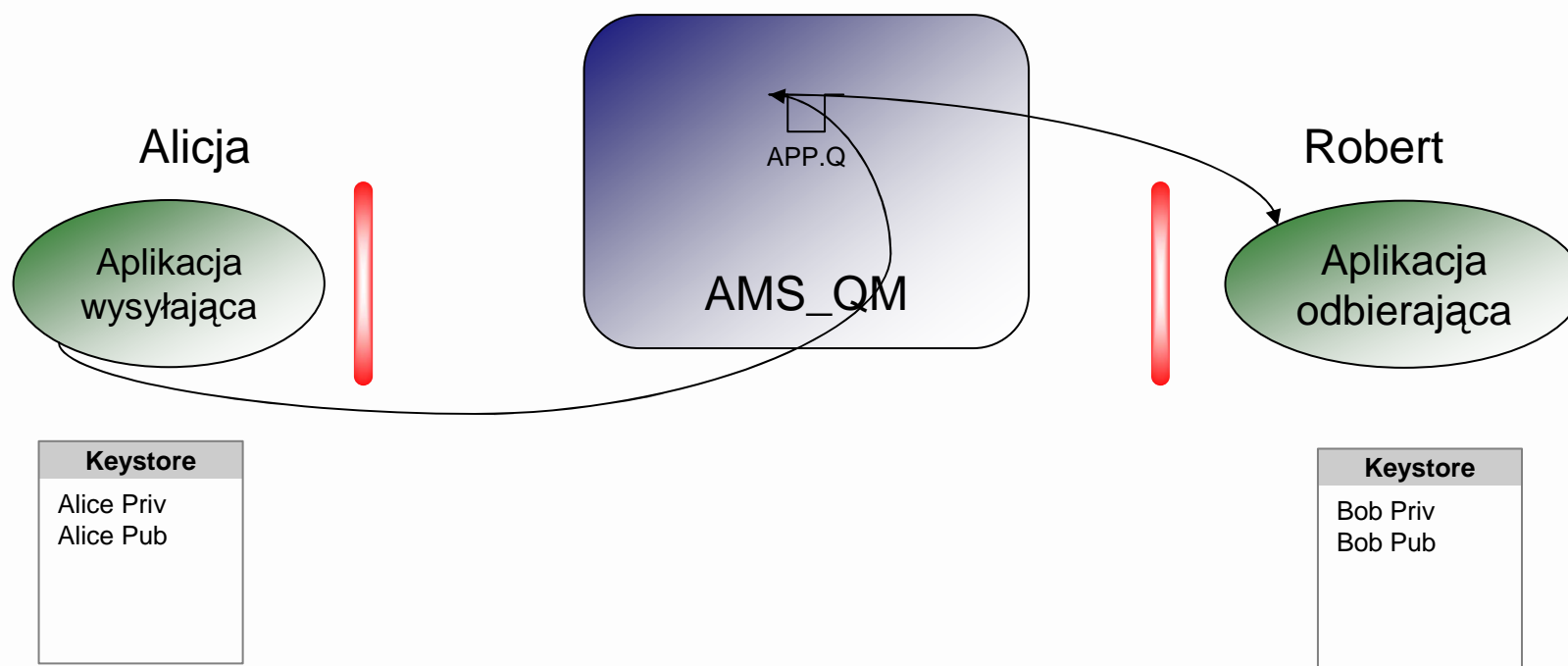
# WebSphere MQ AMS



1. Włączenie WMQ AMS



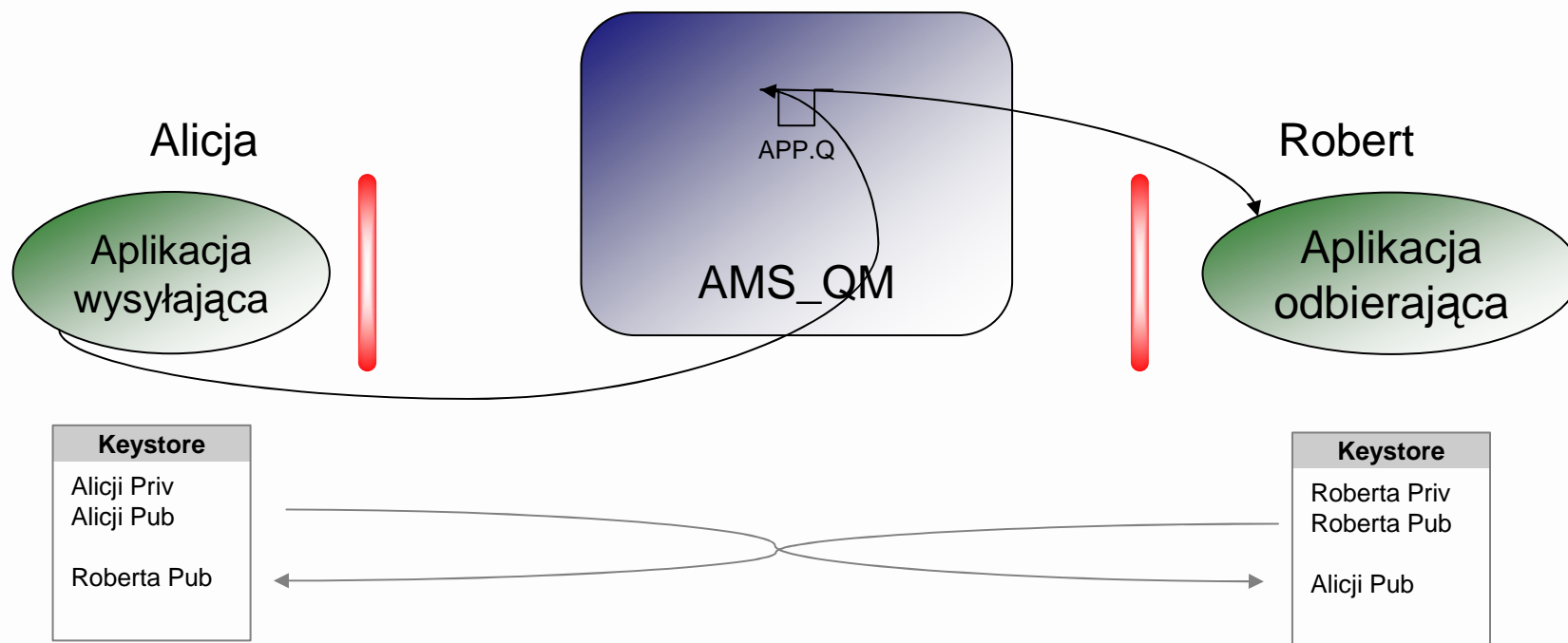
# WebSphere MQ AMS



1. Włączenie AMS
2. Utworzenie pary certyfikat / klucz prywatny



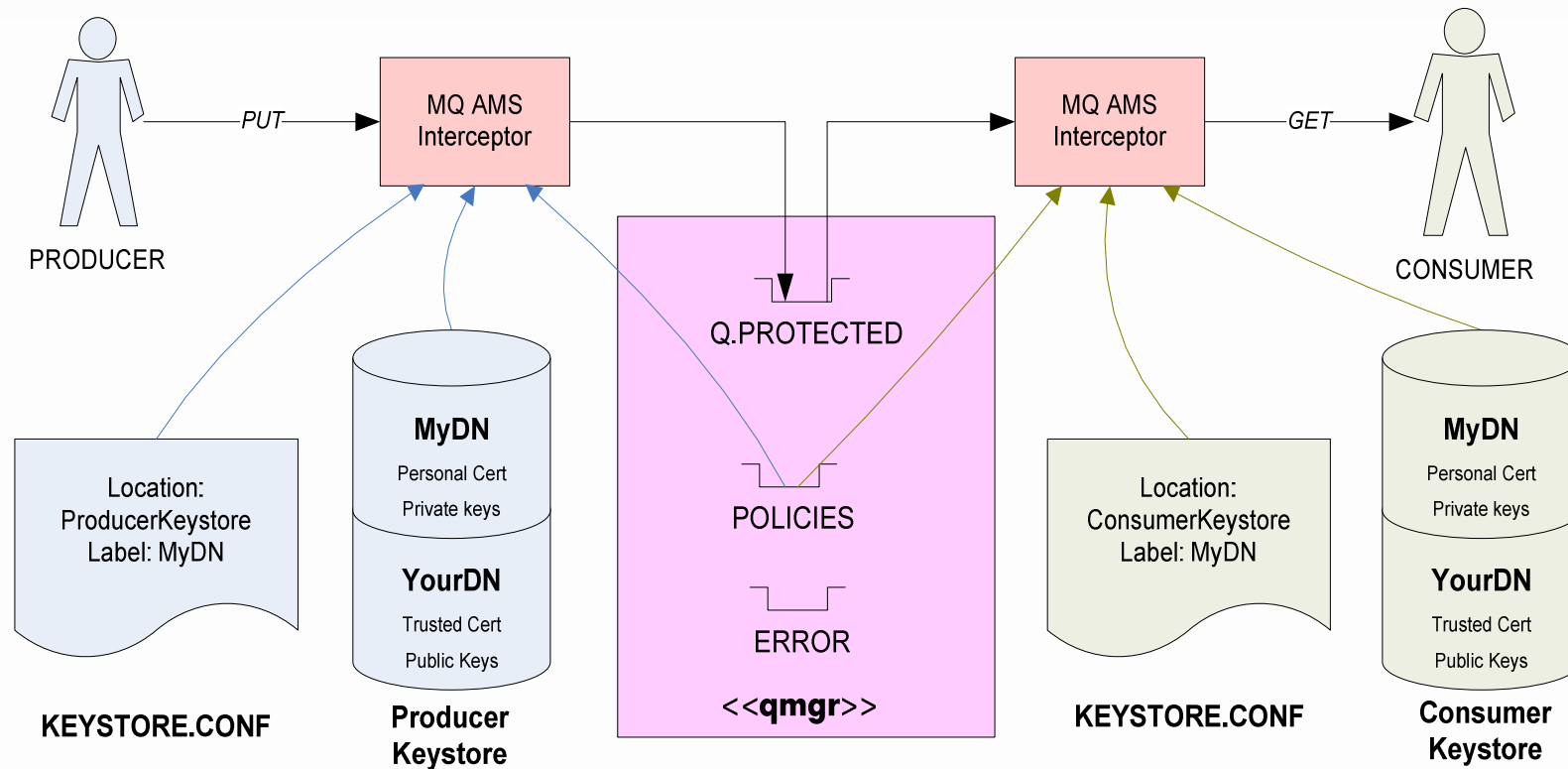
# WebSphere MQ AMS



- Włączenie AMS
- Utworzenie pary certyfikat / klucz prywatny
- Kopia certyfikatu publicznego



# Logiczna architektura



# WMQ AMS – główne cechy



- Zabezpiecza wrażliwe lub bardzo wartościowe komunikaty MQ
- Wykrywa i usuwa nieautoryzowane komunikaty zanim zostaną przetworzone przez odbierające aplikacje
- Sprawdza czy komunikaty podczas podróży pomiędzy kolejkami nie zmieniły treści
- Chroni komunikaty nie tylko podczas przesyłu pomiędzy kolejkami ale również kiedy oczekują w kolejce na pobranie
- Komunikaty z aplikacji MQ są w sposób transparentny zabezpieczane poprzez przerwania
- Zabezpiecza komunikaty punkt-punkt



# Różne polityki bezpieczeństwa



- Tworzenie, usuwanie, modyfikacja za pomocą 'setmqspl'
- Lub przez MQ AMS plug-in for MQ Explorer (GUI).
- Polityki zapisywane do 'SYSTEM.PROTECTION.POLICY.QUEUE'.
- Każda kolejka może mieć tylko jedną politykę.
- Dwa typy polityk:
  - Integralność.
  - Prywatność.
- Wyświetlanie polityk 'dspmqspl'.



# Zalety



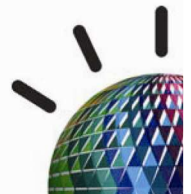
- Zwiększa bezpieczeństwo infrastruktury WMQ
- Zapewnia niepodważalność, niezmiennosc treści i prywatność
- Transparentny dla istniejącej infrastruktury
- Bezinwazyjny dla aplikacji
- Prosty do użycia
- Oparty na otwartych standardach PKI







# WebSphere MQ MFT



# WebSphere MQ MFT



“WebSphere MQ File Transfer Edition”

To obecnie

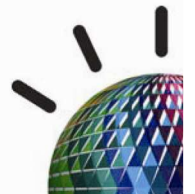
“WebSphere MQ Managed File Transfer”

- The managed file transfer capabilities previously available in the WebSphere MQ File Transfer Edition (FTE) product are now fully integrated into the WebSphere MQ product, and installable via the Managed File Transfer components.

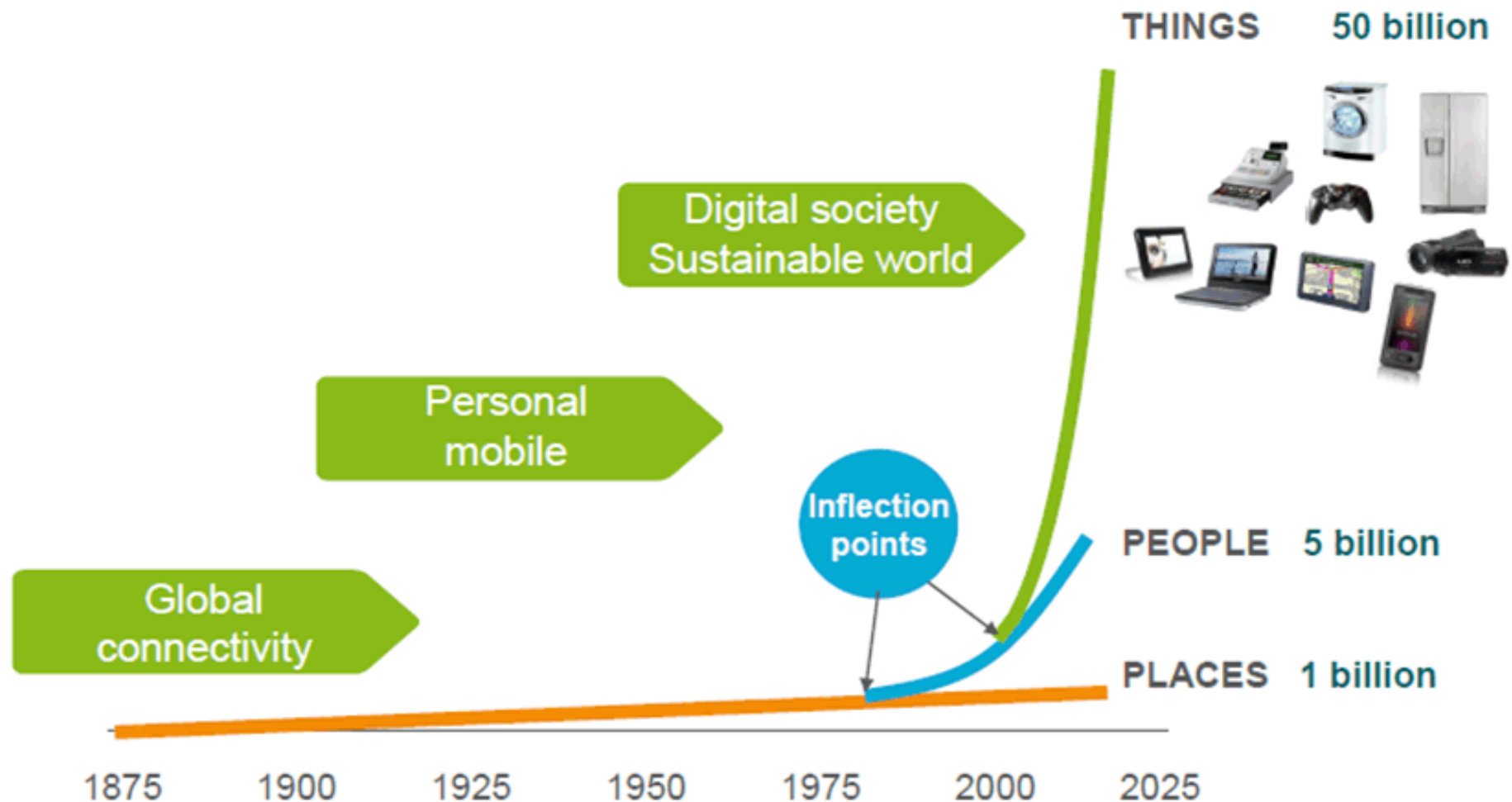




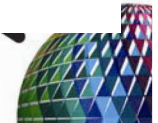
# WebSphere MQ Telemetry



# Eksploracja urządzeń mobilnych



Source: Ericsson AB, "Infrastructure Innovation - Can the Challenge be met?," Sept 2010



# Zmiana zachowań i podejścia



Biurkowy



Mobilny



Używany w domu/pracy

Używany w ruchu

Zorientowany na dokumenty

Zorientowany na komunikaty

Duże złożone aplikacje

Konkretne mini aplikacje

Neutrealne dla kontekstu

Świadome kontekstu

Zadaniowe

Zdarzeniowe

Zasilane z sieci

Zasilane bateriami

Działające w stabilnej sieci

Dostęp do sieci i jej jakość nieznany



# Wymaga zmiany podejścia



## HTML4

- Aplikacje muszą być online
- Wymagane instalowanie dodatkowych wtyczek (e.g., Flash, Silverlight)

## HTML5

- Działają w trybie off-line
- Wtyczki nie są wymagane.

## HTTP

- Nie został zaprojektowany dla niezawodności
  - Straty danych w sieciach o słabej jakości
- Zorientowany na „polling”
  - Wykorzystuje niepotrzebną komunikację
  - Niszczy baterię
- „Rozmowny”
  - Każdy komunikat generuje dużo ruchu
- Jednokierunkowe wywołania
  - Klient zawsze inicjuje komunikację.

## WebSockets?

- Dwukierunkowa wymiana danych
  - Użyteczny na mechanizmu „push” oraz „streamingu”
- **Brakuje podstawowych cech**
  - Wykorzystuje niskopoziomowo TCP a nie jest pełnowartościowym protokołem
  - Brak zapewnienia dostarczenia
  - Nie wspiera publish / subscribe



# Nowe wymagania, inne bezpieczeństwo



## SMS

- Powszechnie używany (wspierany przez każdy telefon/telekom)
- Drogi, opłaty za sms
- Komunikat ograniczony do tekstu
- Otwarta treść (sms czytany przez telekom)

## Dostawcy urządzeń

- Nieprzenaszalny; różny dla różnych urządzeń
  - APNS (Apple), C2DM (Google), BBM (RIM)
- Komunikat ograniczony do tekstu
- Niebezpieczny (dane przesyłane poprzez Google, Apple, RIM)
- APNS/C2DM komunikacja jednokierunkowa



# MQ Telemetry Transport (MQTT)



Minimalizuje użycie sieci

Spodziewa się przerw w działaniu sieci

Działa w sieciach słabej jakości i wolnych

Nie wymaga dużych zasobów i „mocnych” urządzeń

Wykorzystuje mechanizm publish/subscribe

Dostarcza różne poziomy QoS

Dostarcza “otwarty opublikowany protokół”

– Prosty do użycia przez urządzenia i ludzi.





# Przykład wykorzystania MQTT

*DLaczego facebook wykorzystał MQTT dla 350mln użytkowników mobilnych*



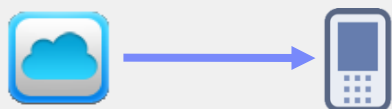
“.. performance improvements designed to make your messaging experience even better. To do this without killing battery life, we used a protocol called MQTT ... designed to use bandwidth and batteries sparingly... phone-to-phone in hundreds of milliseconds, rather than multiple seconds.”

- Lucy Zhang, Facebook Engineer 10/19/11 [www.facebook.com/lucyz](http://www.facebook.com/lucyz)  
(MQTT used by their 350M mobile users, 475 mobile operators)

# Wartość dodana MQTT dla Aplikacji Mobilnych



## „Push” Pytanie/Odpowiedź



- ✓ Alerty On-line
- ✓ Śledzenie
- ✓ Potwierdzenie odbioru

## Niskie koszty



Dobre wykorzystanie pasma sieci



Tańszy niż SMS

## Bogaty szkielet

- ✓ Dwukierunkowy
- ✓ Rich / HTML Messages
- ✓ Bezpieczny
- ✓ Prosty

## Niskie zużycie energii



0.3041%



0.0047%

% Baterii na godzinę



# WebSphere MQ V7.5: Cechy podsumowanie



| <i>Nowa cecha</i>  | <i>Zysk</i>  | <i>Opis</i>   |
|--|--|---|
| <b>Możliwość instalacji wielu wersji MQ na platformach „Distributed”</b> | Łatwiejsza migracja do nowej wersji, z możliwością współistnienia ze starszą | Dla Unix i Windows wsparcie dla wielu wersji MQ V7.x (i jednej kopii MQ V7.0.1) w celu utrzymania różnych fixpack’ów.<br>Wsparcie dla relokacji instalacji.<br>Aplikacje mogą podłączyć się do dowolnego Qmgr |
| <b>Zwiększone bezpieczeństwo</b>   | Uproszczona konfiguracja<br><br>Rozszerzona autoryzacja i audyt              | Autoryzacja w oparciu o adres IP<br><br>Dodatkowe algorytmy kryptograficzne<br><br>Większa granulacja autoryzacji dla innych kolejek niż lokalne<br><br>Raporty aktywności aplikacji                          |
| <b>Wsparcie dla Chmury (Cloud)</b>                                       | Upraszcza i wspiera cloud computing  | Dodatkowe obrazy HVE  |
| <b>Rozszerzenie funkcjonalności Klastra</b>                              | Zwiększona łatwość użycia  | Autoryzacja dla Cluster Q niż dla XMIT Q dla platform Dist.<br><br>Wsparcie łączności - Bind-on-Group   |
| <b>Dostępność Multicast’u</b>  | Nowa jakość (low-latency) dla scenariusza fan-out                            | Dla MQ Pub/Sub wykorzystanie multicast (Group Addresses Provides) i bezpośrednia współpraca z MQ LLM  |
| <b>Zwiększona wydajność</b>  | Lepsze wykorzystanie procesorów wielordzeniowych                             | Wiele zmian w kodzie  |

