

112 Lokalizacja

Prezentacja dla UKE

Andrzej Bartosiewicz, NASK © 2007



Agenda

- Podstawy prawne
- Użyte skróty
- Schemat przepływu danych (obecnie i docelowo)
- Rola CPR
- Możliwości integracji
- „push” kontra „pull”
- Dostęp do systemu
- Architektura i cechy systemu



Aktualne podstawy prawne

- Ustawa Prawo Telekomunikacyjne z dnia 16 lipca 2004 r. art.78 i art. 169
- Ustawa o Państwowym Ratownictwie Medycznym z dnia 8 września 2006 art.25 i art.28

oraz:

- Dyrektywa 98/10/EC „the application of open network provision (ONP) to voice telephony and on universal service for telecommunications in a competitive environment”
- Dyrektywa 2002/22/EC „universal service and users' rights relating to electronic communications networks and services” (art.36)



Andrzej Bartosiewicz
NASK © 2007

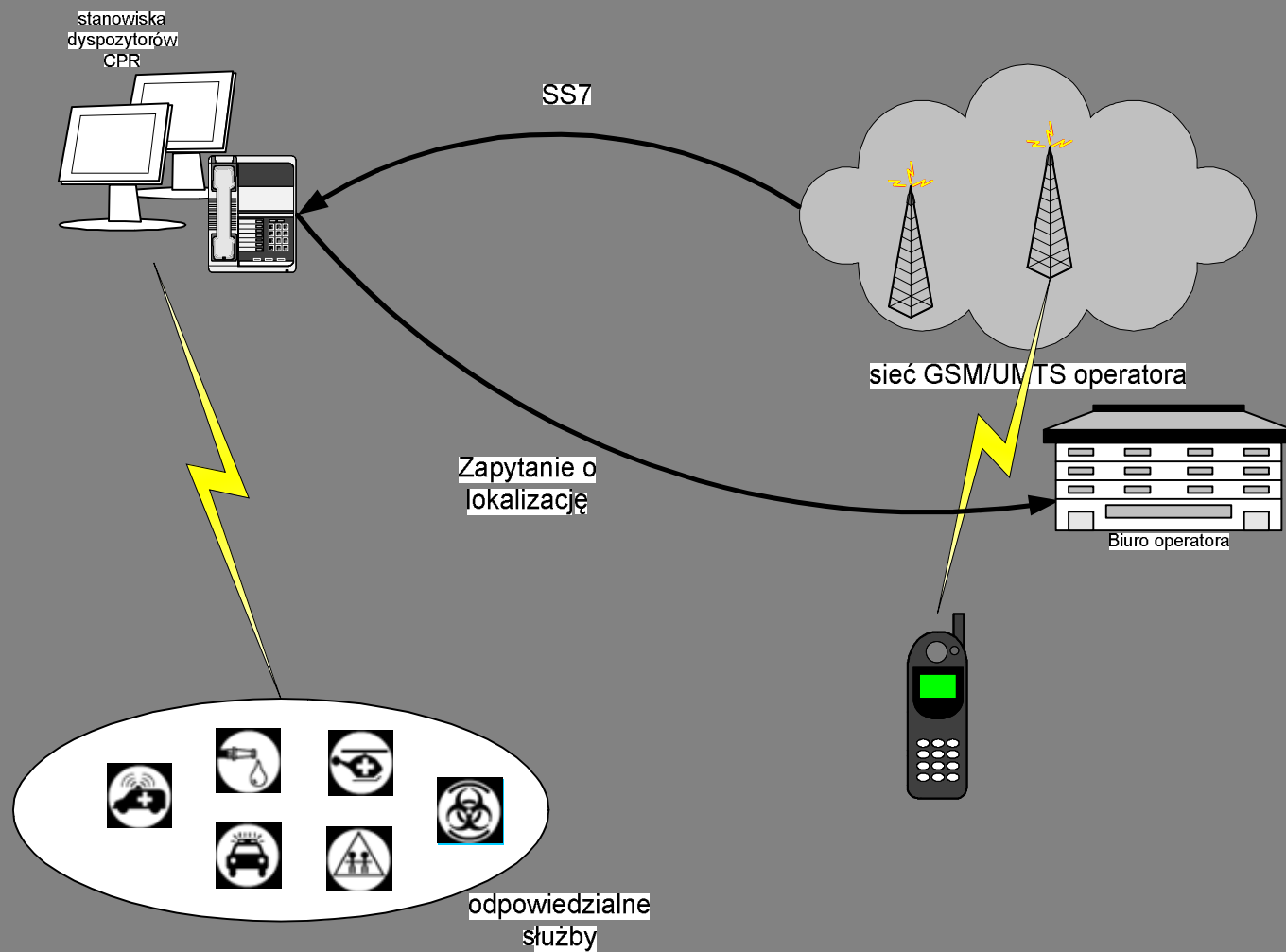
Skróty

ACN:	Automotive Crash Notification
CPR:	Centrum Powiadamiania ratunkowego
DDDS:	Dynamic Delegation Discovery System
EBL:	ENUM Branch Location
ECC:	Emergency Control Center
EPP:	Extensible Provisioning Protocol
ETSI:	European Telecommunications Standards Institute
IP:	Internet Protocol
MLP:	Mobile Location Protocol
NAPTR RR:	The Naming Authority Pointer DNS Resource Record
NP:	Number Portability
NPDB:	Number Portability Database
NRA:	National Regulatory Authority
PSAP:	Public Safety Answering Point
PSTN:	Public switched telephone network
PT:	Prawo Telekomunikacyjne
URI:	Uniform Resource Identifiers
VPN:	Virtual Private network
XML:	Extensible Markup Language

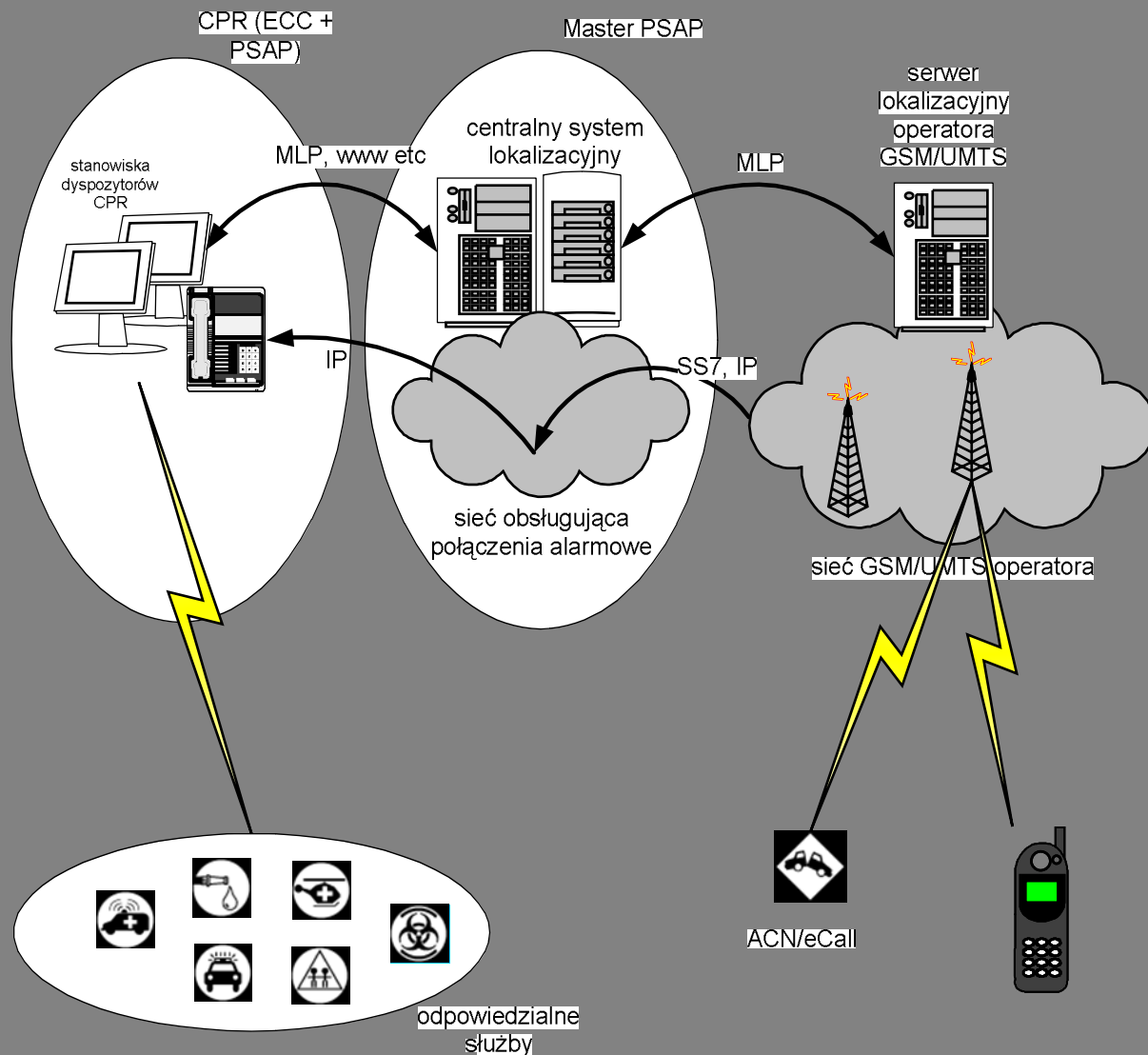


Andrzej Bartosiewicz
NASK © 2007

112: przepływ danych (stan obecny)



112: przepływ danych docelowo



Andrzej Bartosiewicz
NASK © 2007

Przeptyw danych

- Sieć operatora w czasie inicjowania połączenia 112 zestawia (wg. normy ETSI TS 102 164) połączenie z *Public Safety Answering Point (PSAP)* gdzie następuje przekierowanie połączenia do *Emergency Control Center (ECC)*.
- W momencie zestawiania połączenia, następować powinno (obok zestawienia faktycznego połączenia głosowego) przesłanie informacji lokalizacyjnej o umiejscowieniu Abonenta do serwera lokalizacyjnego w sieci operatora, skąd informacja o lokalizacji powinna trafić do centralnego systemu odpowiedzialnego za zarządzanie tymi danymi wg standardu protokołu ETSI TS 102 164
- Następnie informacja trafia do ECC z wykorzystaniem dowolnego lokalnego rozwiązania – niekoniecznie zgodnego ze standardami ETSI

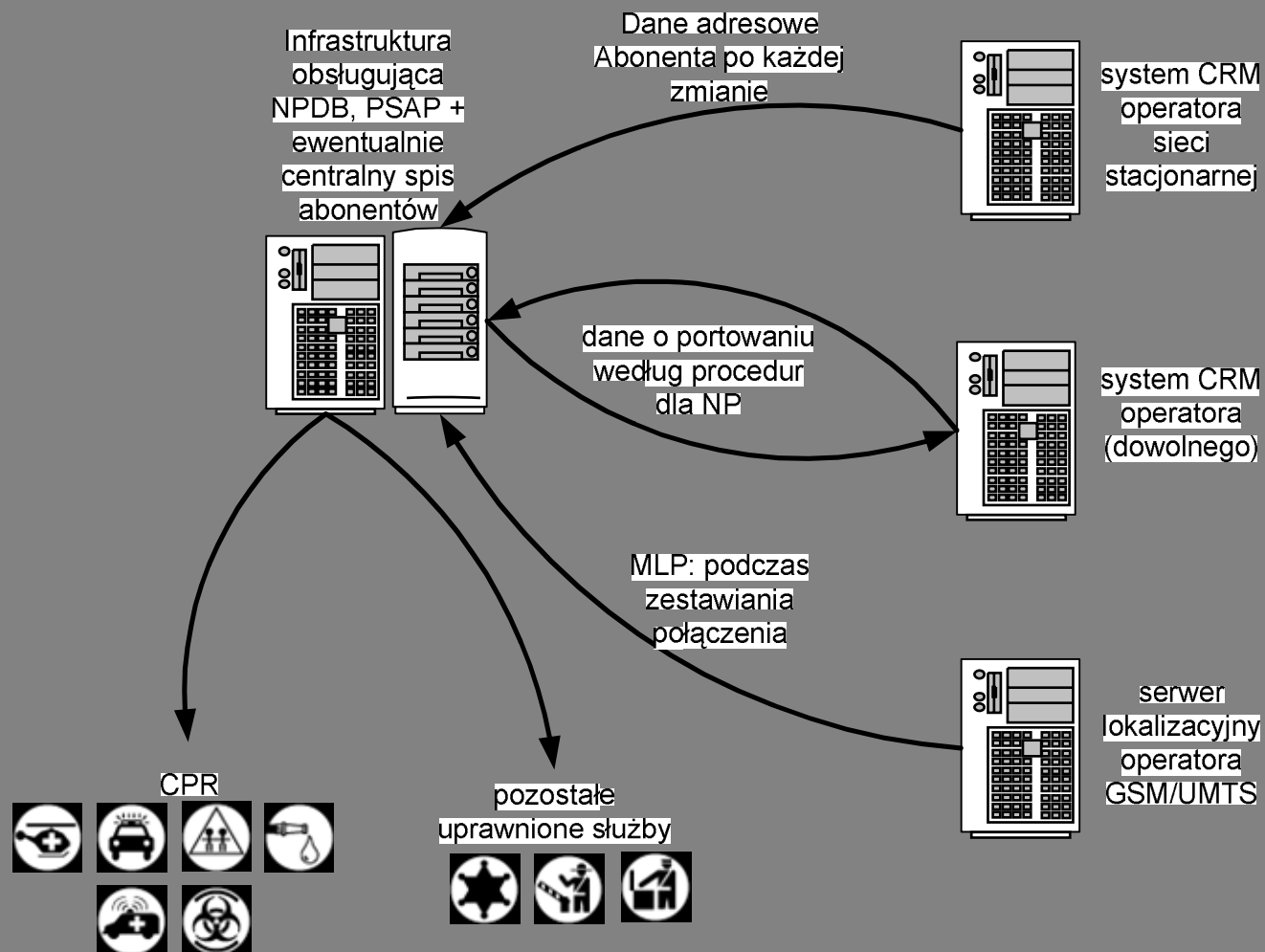


Rola CPR

- Zakładając że w warunkach polskich istnieje będzie ponad 100 tzw. Centrów Powiadamiania Ratownictwa (CPR), powinniśmy przyjąć, że rolę ECC / PSAP będą stanowiły CPR, które niekoniecznie muszą dysponować pełną infrastrukturą pozwalającą na samodzielną lokalizację na mapach.
- Centralny system lokalizacyjny w „Master PSAP” może przekazywać do mniej zaawansowanych technicznie CPR dane w postaci wstępnie przetworzonej mapy z zaznaczoną lokalizacją Abonenta (możliwa opcja).
- Bardziej zaawansowane CPR mogą pobierać dane w postaci niezmienionej (ETSI TS 102 164; MLP) i same dokonywać transformacji danych lokalizacyjnych na postać prezentacyjną (preferowana opcja).



Możliwość integracji usług



Andrzej Bartosiewicz
NASK © 2007

Integracja usług - zalety

- W rozwiązaniu tym centralna baza numerów przeniesionych (NPDB) zintegrowana jest z bazą lokalizacyjną PSAP. Ważnym elementem tego rozwiązania jest nie tylko integracja NPDB z PSAP, ale także fakt, że po stronie operatorów wykorzystywany jest jeden protokół komunikacyjny ze zintegrowanym systemem oraz te same zabezpieczone kanały komunikacyjne (np. VPN).
- Dodatkowo (teoretycznie – obecnie ustawa PT nie zakłada takiego rozwiązania), dane z systemów mogą służyć jako centralny ogólnokrajowy spis abonentów na potrzeby informacyjne oraz potrzeby uprawnionych służb (np. Policja, ABW, CBA, CBS).
- Dzięki integracji obu systemów, możliwa jest znaczna redukcja kosztów rozwiązania nie tylko po stronie operatorów (jeden interface, te same zabezpieczenia, certyfikaty, kanał komunikacyjny etc.), ale przede wszystkim administracji rządowej w zakresie zakupu i utrzymania (kolokacja, administracja) infrastruktury (serwery, urządzenia sieciowe, łącza, software) wraz z centrum zapasowym.



„push” czy „pull”?

- Rozwiązaniem optymalnym jest istnienie centralnej bazy danych lokalizacyjnych w której przechowywane są dane lokalizacyjne abonentów sieci stacjonarnych oraz odnotowywane są dane o lokalizacji abonentów komórkowych w momencie zestawiania połączenia (metoda „push”).
- W zakresie połączeń komórkowych można też rozważyć jako wariant przejściowy metodę „pull”, a więc przekazywanie przez operatora danych lokalizacyjnych na żądanie CPR (dyspozytor ECC poprzez „Master PSAP”). W takiej jednak sytuacji PSAP musi posiadać informację który z operatorów jest właściwy dla danego numeru, a więc posiadać możliwość sprawdzenia w bazie numerów przeniesionych który z operatorów aktualnie obsługuje Abonenta dzwoniącego na 112.

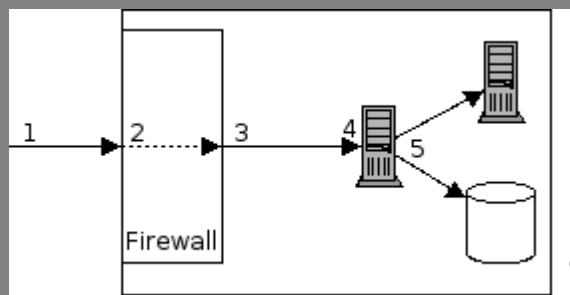


Dostęp do systemu (1)

Platforma pozwala na wykorzystanie istniejących mechanizmów dostępu do zgromadzonych danych przez upoważnione podmioty, można bowiem wyobrazić sobie trzy modele uzyskiwania danych z systemu (podlegające tym samym ograniczeniom dostępu):

- oparty o wyspecjalizowany protokół (najlepiej ten sam czyli EPP – stosowany przez operatorów dla celów przekazywania danych do systemu) wspierający XML
- prezentację przez strony WWW danych tekstowych lub wygenerowanych map z zaznaczonymi miejscami incydentów (dla CPR o najmniejszym poziomie zaawansowania; zapewne wypierany stopniowo przez dwa pozostałe mechanizmy)
- oparty o mechanizmy DNS czyli mechanizm ENUM jako najbardziej otwarty protokół (rozwiązanie optymalne dla operatorów VoIP)





Dostęp do systemu (2)

W pierwszej etapie połączenie przechodzi przez firewall (oznaczony numerem 2) dedykowany dla systemu. Na firewallu na podstawie jego konfiguracji oraz danych na temat połączenia, jest podejmowana decyzja czy je przyjąć czy odrzucić. W przypadku akceptacji tego połączenia, następuje jego wpuszczenie do sieci wewnętrznej (numer 3). W następnym kroku następuje negocjacja certyfikatów (oznaczona numerem 4). Na tym etapie, aby zostać przepuszczonym dalej, połączenie operatorskie, musi się przedstawić pasującym do niego certyfikatem, który został podpisany (uwierzytelniony) przez certyfikat, którym przedstawia się system.

Dzięki temu:

- Weryfikujemy połączenie operatorskie jako uprawnione do przedstawienia się danym certyfikatem (musi on pasować do parametrów tego połączenia)
- Operator weryfikuje czy podłącza się do właściwego systemu (nikt się nie podszywa pod taki system, aby wykraść lub podejrzec dane wysyłane przez operatora)
- Po przejściu powyższego kroku, wszystkie dane przesyłane przez obie strony do siebie, są szyfrowane mocnym algorytmem, uniemożliwiając tym samym wykradzenie przesyłanych danych (ataki typu "man-in-the-middle")
- W ostatnim etapie (oznaczonym numerem 5), operator połączenia autoryzuje się np. za pomocą loginu i hasła w usłudze, do której chce mieć dostęp



Andrzej Bartosiewicz
NASK © 2007

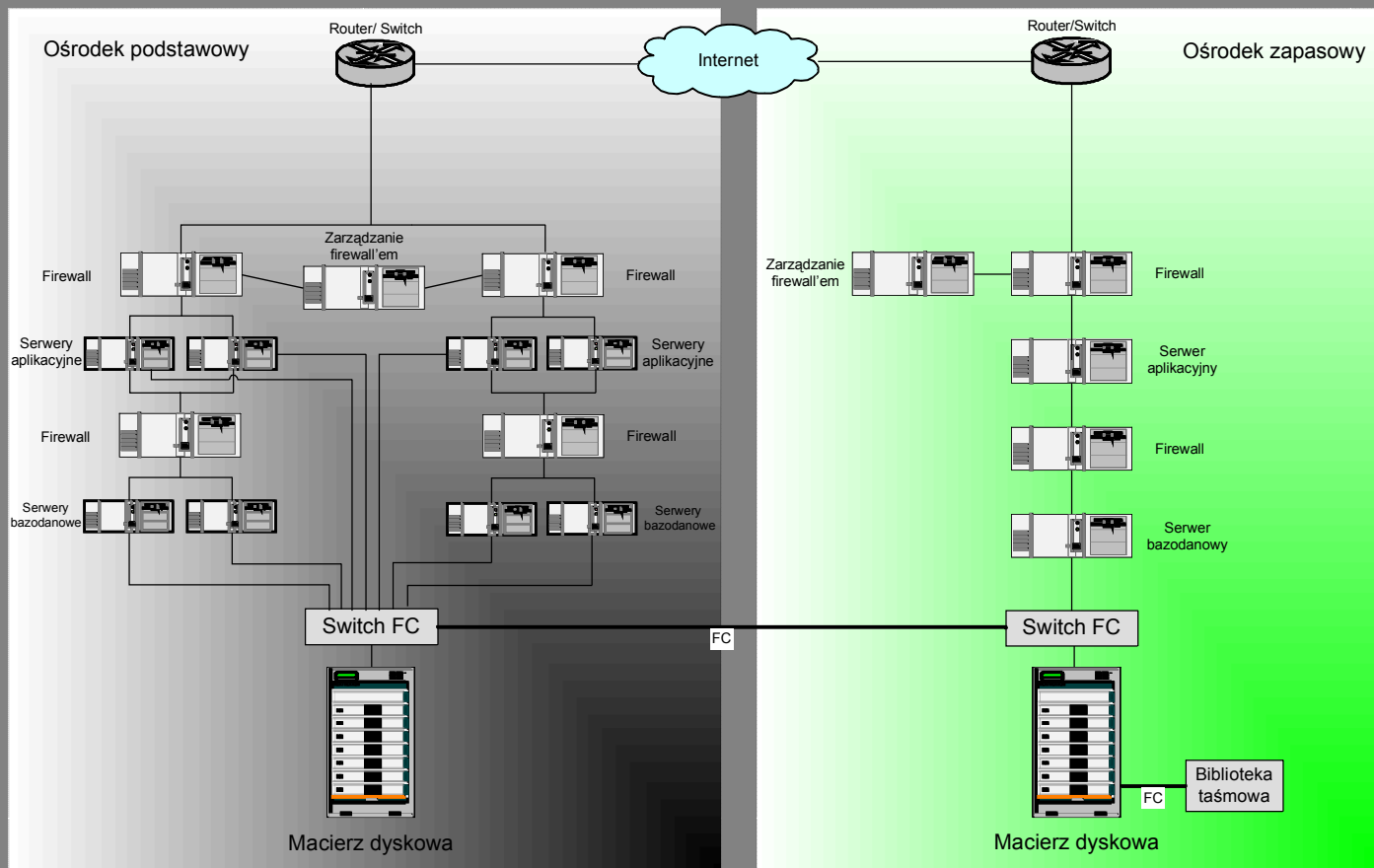
Cechy systemu

Zakłada się bezpieczne przechowywanie i udostępnianie danych, spełniając następujące wymagania:

- **Skalowalność** – łatwa i szybka rozbudowa systemu bez przerywania jego pracy poprzez m.in. budowę wielowarstwową, komponentową pozwalającą na rozdzielanie podstawowych funkcji systemu
- **Wydajność** - odporność na zwiększone (nagłe i nieprzewidziane) obciążenie systemu oraz możliwość rozbudowy w kierunku balansowania obciążenia
- **Niezawodność** – zapewniona ciągłość świadczenia serwisu
- Wysoki poziom dostępności systemu (**high availability**) poprzez zabezpieczenie w postaci redundantnego centrum zapasowego oraz odporność na awarie pojedynczych elementów rozwiązania
- Gwarantowany maksymalny czas odpowiedzi na zapytania przy określonych założeniach maksymalnej ilości odpytań jednoczesnych



Schemat logiczny systemu



Dane w zaproponowanej architekturze systemu będą replikowane pomiędzy macierzami dyskowymi znajdującymi się w różnych ośrodkach w sposób synchroniczny z użyciem mechanizmu wewnątrz macierzowego wykorzystując zdublowane łącza światłowodowe (dwie różne drogi). System byłby objęty odpowiednią polityką backup'u i archiwizacji danych realizowaną z użyciem biblioteki taśmowej. W przypadku awarii ośrodka podstawowego, ruch automatycznie zostanie skierowany do ośrodka zapasowego.



Andrzej Bartosiewicz
NASK © 2007

Replikacja w DNS

Dodatkowym argumentem wykorzystania platformy ENUM jest możliwość zapewnienia redundancji danych bez konieczności stosowania komercyjnych, skomplikowanych zewnętrznych mechanizmów replikacyjnych (na poziomie sprzętowym lub bazodanowym) pomiędzy Master PASP a CPR.

Bazodanowe mechanizmy replikacyjne będą stosowane na poziomie centralnej bazy danych



Andrzej Bartosiewicz
NASK © 2007

A black and white photograph of a snowy landscape. A path or road is covered in snow, leading towards the horizon. On the right side of the path, there is a line of utility poles with cross-arms and wires. The sky is overcast and grey. The overall scene is desolate and wintry.

Andrzej Bartosiewicz
Kierownik Działu Domen NASK

andrzejb@NASK.pl
skype: abartosiewicz