X.500 — STANDARD I USŁUGI KATALOGOWE*

Maja Górecka **Tomasz Wolniewicz**†

Naukowa i Akademicka Sieć Komputerowa
Bartycka 18, 00–716 Warszawa‡

1 Wstęp

Dynamicznie rosnąca popularność sieci Internet pociąga za sobą konieczność rozwoju nowych aplikacji w celu elastycznej adaptacji oferowanych usług do potrzeb przeciętnego użytkownika.

Masowa ilość informacji potencjalnie dostępnej w Internecie powinna być w sposób niezawodny dostarczana do użytkownika, niezależnie od miejsca jej rezydencji. Niezmiernie istotne jest więc funkcjonowanie sieci rozproszonych baz danych, które uproszczą odzyskanie pożądanej informacji. W tym celu m.in. został zaimplementowany standard OSI — protokół X.500, definujący dostęp do rozproszonej bazy danych (X.500 Directory).

Celem niniejszego artykułu jest przybliżenie tematyki związanej z pojęciem X.500 Directory. Pomimo, że termin X.500 zaczyna się coraz częściej pojawiać w opracowaniach związanych z Internetem, wielu specjalistów zajmujących się usługami sieciowymi ma jedynie pobieżną wiedzę na ten temat. Prace prowadzone ostatnio w zakresie WHOIS++ mogą być odbierane jako atak na X.500, nie brakuje też głosów krytyki pod adresem samego standardu. Postaramy się poniżej pokazać czym jest X.500, na ile może być użyteczne, jaki jest jego związek z innymi usługami sieciowymi.

Przedstawiamy również w skrócie prace prowadzone w zakresie polskiego pilotowego projektu X.500.

Na zakończenie czytelnik znajdzie krótką informacje na temat rozszerzeń standardu zawartych w jego nowej (nieopublikowanej jeszcze) wersji.

Dużym problemem przy pisaniu o X.500 jest brak ustalonego słownictwa. Pierwszym poważnym kłopotem jest przetłumaczenie samego słowa *Directory*, czy określenia *Directory Services*. W wielu przypadkach terminu *Directory* w ogóle nie tłumaczymy, w innych stosujemy określenia *katalog*, czy *usługi katalogowe*.

---

*Prace wykonano w ramach działalności statutowej NASK.

†Adresy autorów: M. Górecka: Ogólnouczelniany Ośrodek Obliczeniowy, UMK Toruń, T. Wolniewicz: Wydział Matematyki i Informatyki, UMK Toruń

‡Autorzy pragna w tym miejscu podziekować mgr. inż. Jerzemu Żenkiewiczowi, który z ramienia NASK koordynuje prace w zakresie X.500, za kilkuletnia współprace i wsparcie naszych działań. Panom prof. Jerzemu Brzezińskiemu i dr Tomaszowi Koszlajdzie dziekujemy za pomoc w zakresie teorii baz danych i uspójnienie naszej wiedzy. Poparcie NASK umożliwiało nam prowadzenie prac oraz branie udziału w europejskich spotkaniach koordynacyjnych X.500

2 X.500 jako standard CCITT/ISO

Standard CCITT X.500/ISO 9594 z 1988 roku definiuje rozproszoną bazę danych przeznaczoną przede wszystkim dla celów szeroko rozumianej informacji adresowej. Na pierwszej stronie oficjalnego tekstu [1] czytamy: *Directory udostępnia usługi katalogowe wymagane przez aplikacje OSI, procesy zarządzania standardu OSI, elementy innych warstw OSI oraz usługi telekomunikacyjne. [...] Directory nie jest pomyślane jako baza danych ogólnego przeznaczenia, pomimo że może być tworzona w oparciu o takie systemy. Na przykład, zakłada się, że podobnie jak dla katalogów komunikacyjnych, częstotliwość „zapytań" jest wyraźnie wyższa od częstości poprawek.*

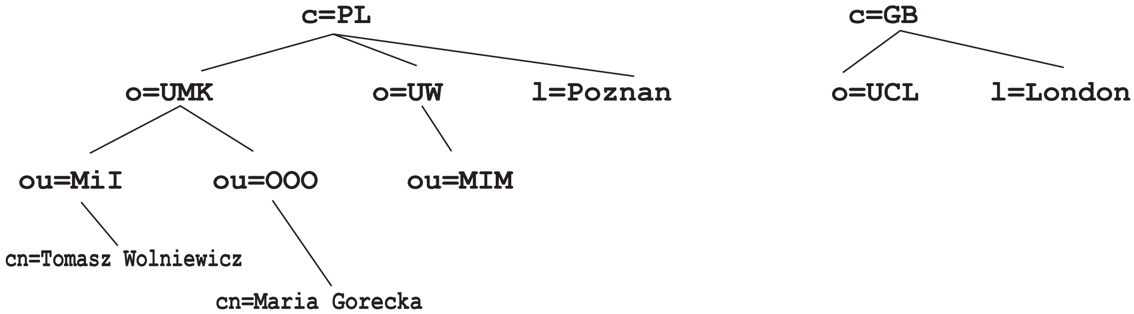
Standard opisuje:

- **Model Bazy** (Directory Model), a w jego zakresie:
  - **Model funkcjonalny** — określenie zasad działania bazy — sposobu dostępu, komunikacji między klientem i serwerem oraz samymi serwerami,
  - **Model organizacyjny** — określenie zasad zarządzania bazą podzieloną na tzw. *Domeny Zarządzania* (Directory Management Domain — DMD),
- **Model informacyjny** (Information Model) — określenie odwzorowania opisywanej rzeczywistości na elementy bazy danych,
- **Model bezpieczeństwa** (Security Model) — założenia systemu autoryzacji dostępu,
- Określenie protokołów komunikacji.

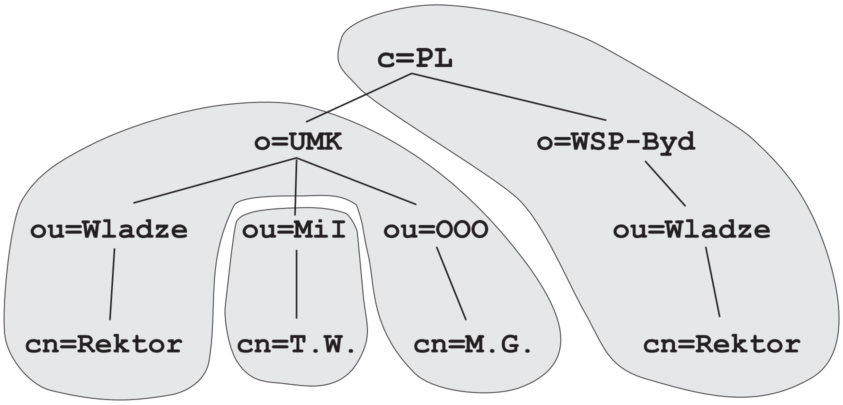
W dodatkach, nie będących formalnie składową samego standardu, opisuje się przykładowy zestaw atrybutów i typów obiektów przechowywanych w X.500. Ustalenia zawarte w dodatkach miały na celu ułatwienie budowy spójnych i wzajemnie kompatybilnych implementacji w oparciu o jednolity schemat wymiany danych.

W ramach modelu informacyjnego określa się, że rzeczywistość, przedstawiana jako zbiór obiektów opisywanych atrybutami i nazywanych Directory Information Base (DIB), odwzorowywana jest na drzewiastą strukturę o nazwie Directory Information Tree (DIT). Podstawowymi elementami DIT są obiekty takie jak kraj, instytucja, jednostka organizacyjna, jednostka geograficzna, osoba, ale może to być również dokument, usługa komputerowa itp.

Przykładowy wycinek DIT może wyglądać następująco:



Podstawowymi elementami modelu funkcjonalnego są **serwery** (**DSA** — Directory System Agent) oraz oprogramowanie klienckie (**DUA** — Directory User Agent). Każdy DSA „panuje" nad pewnym wycinkiem drzewa informacji. Spójne fragmenty drzewa informacji nazywane są kontekstami (Naming Context), w typowej sytuacji DSA zarządza pojedynczym kontekstem. Przykłady kontekstów pokazane są na rysunku poniżej.



Każdy DSA, z wyjątkiem DSA najwyższego poziomu, musi znać metodę dostępu do DSA zarządzającego kontekstem bezpośrednio powyżej, jak również do DSA zarządzających kontekstami bezpośrednio poniższymi. Taka organizacja bazy pozwala na dostęp do dowolnego fragmentu drzewa za pomocą jednej z dwóch metod: **odesłania** (referral) — przekazania informacji o kolejnym DSA, który może być „bliższy" poszukiwanej informacji, lub **tworzenia łańcuchów** (chaining) — wykonania połączenia w imieniu pytającego i przekazania gotowej informacji. To, który wariant zostanie wybrany zależy od paremetrów konfiguracyjnych, opcji zapytania, jak również możliwości dokonania bezpośredniego połączenia przez pytającego (w pewnych sytuacjach DSA pośrednie może pełnić rolę pomostu pomiędzy sieciami).

Każdy obiekt występujący w DIT jest jednoznacznie charakteryzowany przez swoją **Nazwę Wyróżnioną** (Distinguished Name) składającą się z ciągu nazw węzłów gałęzi drzewa DIT prowadzącej do opisywanego obiektu. Ostatni człon DN nazywany jest **Relatywną Nazwą Wyróżnioną** (Relative Distinguished Name), DN jest zatem ciągiem RDN. Przykładowo DN może wyglądać:

```
c=PL@o=Uniwersytet Mikolaja Kopernika@ou=Wladze@cn=Rektor
```

Znak `@` jest używany do oddzielania RDN w ramach DN.

Obiekty bazy X.500 muszą być określonych typów nazywanych po angielsku **Object Class**. Typ zawiera opis atrybutów, które dany obiekt musi posiadać, jak również tych, które są opcjonalne. Z atrybutami związane są ich typy. W trakcie komunikacji pomiędzy DSA zachodzi konieczność przekazywania typów obiektów i wartości atrybutów. Atrybuty przekazywane są jako pary `(nazwa atrybutu, wartość atrybutu)`. Zarówno typy obiektów jak i nazwy atrybutów oznaczane są jednoznacznymi identyfikatorami i te, a nie nazwy, są w istocie przesyłane w sieci (wykorzystuje się w tym celu standard ASN.1 i zwiazanie z nim metody kodowania BER). W przypadku zdefiniowania lokalnych typów, czy atrybutów, przyporządkowuje się im nowe identyfikatory. W konsekwencji „obce" DSA i DUA nie są w stanie tych elementów interpretować. Przy zachowaniu zasady, że każdy obiekt posiada pewne atrybuty standardowe nie zachodzi obawa, że nie zostanie on w ogóle odczytany, a równocześnie jednoznaczność identyfikatorów gwarantuje, że nieznane identyfikatory nigdy nie zostaną zinterpretowane błędnie. Ta możliwość rozszerzania jest wykorzystywana między innymi przy dostosowywaniu bazy do lokalnego języka, o czym piszemy w części 4.4.

3 X.500 jako usługa sieciowa

Sprawdzenie funkcjonalności modelu opisanego w standardzie X.500 było niemożliwe bez uruchomienia pilotowej bazy danych o znacznym stopniu rozproszenia i zauważalnej zawartości. W związku z tym w roku 1990 uruchomiono dwa równoległe i wzajemnie skoordynowane projekty:

White Pages w USA i PARADISE w Europie Zachodniej. W ramach projektów utworzono pilotowe bazy danych w zakresie środowiska akademickiego. Finansowanie centralne pozwalało na utrzymywanie serwera koordynującego informację o pierwszym poziomie drzewa, stanowiska pomocy dla administratorów krajowych, organizację spotkań administratorów. Udział w projekcie był dobrowolny i wolny od opłat. Podłączanie kolejnych krajów następowało po uruchomieniu w danym kraju pierwszego serwera pełniącego rolę koordynującą. Funkcjonowanie bazy oparte było niemal w całości o oprogramowanie ISODE/QUIPU rozpowszechniane nieodpłatnie.

Rozwój projektu był bardzo różny w różnych krajach. W niektórych utworzono stosunkowo kompletne bazy o dużym stopniu użyteczności (np. w Holandii doprowadzono do sytuacji, w której każda instytucja podłączona do akademickiej sieci SurfNet prowadzi własny serwis X.500). Niektóre instytucje uruchomiły niezawodny serwis X.500 wykorzystywany bardzo intensywnie do celów lokalnych. W wielu krajach napotkano jednak na znaczne kłopoty (bardzo często natury formalnej) i tam X.500 jest bardzo ubogie.

Obecnie koordynacja projektu PARADISE została przejęta przez DANTE i prowadzona jest na niedokładnie jeszcze określonych zasadach odpłatności krajów członkowskich. DANTE stawia sobie za cel doprowadzenie do bardziej spójnego obrazu informacji w DIT i dostarczenie niezawodnego serwisu.

Koordynacja usługi takiej jak X.500 jest dosyć specyficzna, sprawne działanie bazy opiera się na wielu ustaleniach administracyjnych, niekiedy pozastandardowych, i w związku z tym niezbędne są, na przykład, stosunkowo częste zebrania koordynacyjne administratorów krajowych. Działalność ta wzmaga się zwłaszcza obecnie, w obliczu przygotowań do wprowadzania nowego standardu X.500. Fakt ten, jak również to, że implementacje X.500 są dosyć wymagające sprzętowo oznacza, że X.500 jest stosunkowo drogie w eksploatacji. Do wspomnianych kosztów dochodzą też koszty utrzymania samej bazy danych, o trudnościach z tym związanych piszemy w części 4.2.

Poza projektem PARADISE/White Pages spore znaczenie może mieć plan kilku europejskich PTT tworzących program Eurascom. Projekt ten ma zbadać skuteczność X.500 jako bazy adresowo-telefonicznej dla celów tych instytucji. Założenia i funkcjonowanie projektu jest jednak utrzymywane w tajemnicy.

3.1 Udział Polski w programie PARADISE

Polska przystąpiła do projektu PARADISE w lecie 1992 roku uruchamiając pierwszy serwer na UMK w Toruniu. Krótko potem patronat nad polskim X.500 przejął NASK. Działania początkowo ograniczały się do wprowadzenia niewielkiej ilości danych, z czasem UMK umieściło swój pełny skład osobowy.

W roku 1994 KBN przyznał dofinansowanie na uruchomienie pilotowej bazy danych w wybranych ośrodkach w Polsce. W rezultacie mamy obecnie pięć aktywnych regionów: Kraków, Poznań, Toruń, Warszawa i Wrocław. W każdym z nich działa serwer regionalny utrzymujący kompletną bazę danych o przynajmniej jednej reprezentatywnej uczelni regionu. Dodatkowo w ramach wspomnianego dofinansowania pozyskano dane z MEN oraz Ośrodka Przetwarzania Informacji w Warszawie. Dane te pozwoliły na umieszczenie informacji o znacznej części kadry naukowej ze stopniem naukowym doktora, jak również o strukturze organizacyjnej polskich uczelni. W chwili obecnej baza liczy ponad 50000 haseł. Mamy nadzieję, że możliwe będzie zdobycie finansowania pozwalającego na utrzymanie obecnych zasobów oraz objęcie zasięgiem projektu znacznie większej liczby ośrodków.

Od 1994 prowadzimy w ramach NASK prace badawczo-rozwojowe dotyczące X.500. Obejmują one ocenę efektywności rozproszonej bazy danych oraz stosowanie znaków diakrytycznych w systemach baz danych X.500 Directory.

3.2 Implementacje X.500

X.500 określa standard, według którego producenci powinni tworzyć swoje oprogramowanie. Implementacji jest stosunkowo niewiele, ale zaczynają się pojawiać w coraz większej liczbie. Od dawna dostępna była implementacja o nazwie QUIPU stanowiąca fragment pakietu ISODE. Oprogramowanie to było przez wiele lat oferowane bez żadnych ograniczeń. Obecnie na bazie ISODE rozpowszechnia się dwa najważniejsze produkty X.500 (wersja firmy NEXOR i wersja ISODE Consortium). Od wielu lat dostępny jest też produkt francuski o nazwie Pizarro, w oparciu o który funkcjonuje francuski pilot.

Sośród innych produktów można wymienić: UCOM X.500, DEC X.500, DIR.X itd. Pełną listę można znaleźć w RFC1632 [3].

4 X.500 w praktyce

4.1 Zalety i wady

X.500 jako baza danych, w praktycznym zastosowaniu ma zarówno zalety jak i pewne wady. Nie ulega wątpliwości, że jedną z największych zalet X.500 jest dostosowanie modelu informacyjnego do przechowywania struktury organizacyjnej instytucji. Odwzorowanie jest całkowicie naturalne i nie wymaga od administratora żadnego specjalnego modelowania.

Kolejną zaletą jest łatwość lokalnego, dynamicznego modelowania struktury przechowywanej informacji przy jednoczesnym zachowaniu spójności bazy w zakresie międzynarodowym. Jest to możliwe dzięki zastosowaniu drzewiastej struktury identyfikatorów, które przyporządkowywane są wszelkim elementom składowym konstrukcji bazy. Jak już wspominaliśmy elementami takimi są typy przechowywanych obiektów, nazwy atrybutów itp. Admninistratorzy lokalni mogą wzbogacać strukturę na swój własny sposób; poza obszarem lokalnym ich modyfikacje nie będą po prostu rozpoznawane, informacja o charakterze uniwersalnym będzie jednak nadal skuteczna. Zasada, z którą się tutaj spotykamy jest identyczna do stosowanej przy konstrukcji MIB dla SNMP (w istocie w obu przypadkach stosuje się takie same identyfikatory).

Po stronie wad na ogół przytacza się powolny wzrost objętości bazy, porównuje się rozwój X.500 z lawinowym rozwojem *gophera* czy *WWW*, jak również z szybkim i niezawodnym działnieniem DNS. Bardzo interesujące poglądy na ten temat można znaleźć w referacie [12], są one zgodne z naszymi własnymi doświadczeniami z pracy przy administrowaniu X.500. Zanim zacznie się na poważnie rozważać wspomniane porównania trzeba sobie zdać sprawę z kilku faktów:

1. X.500 funkcjonuje przede wszystkim jako baza danych o osobach, oznacza to, że zbieranie danych musi być obarczone trudnościami prawnymi i organizacyjnymi. Trudności te napotka każdy system, który będzie próbował zebrać podobne dane.

2. *gopher* i *WWW* nie są bazami danych w sensie teorii takich systemów, są jedynie zbiorowiskiem informacji, którą można przeglądać, ale w ramach której bardzo trudno jest cokolwiek wyszukać. Służby indeksujące są bardzo niepełne. Informacja nie ma żadnej określonej struktury.

3. DNS jest sprawnie funkcjonującym systemem odwzorowywania nazw i adresów na siebie. Ilość informacji, którą przechowuje jest stosunkowo niewielka, nie zawiera żadnych mechanizmów wyszukiwania i bardzo ograniczone mechanizmy „listingu”. DNS jest ponadto absolutnie niezbędny do transportu poczty elektronicznej i z tego powodu każdy administrator dba o aktualność podstawowych danych. W przeciwieństwie do tego X.500 jest usługą dla

świata zewnętrznego i jeżeli użytkownicy nie zaczną domagać sie sprawnego systemu informacji adresowej, przeciętni administratorzy systemów komputerowych nie będą widzieli potrzeby utrzymywania tej bazy jako jednego z priorytetowych zadań.

4. Wielokrotnie podkreślana złożoność X.500 (zarówno samego standardu jak i protokołu) bierze się stąd, że użytkownicy mają bardzo różnorodne wymagania dotyczące rodzaju wprowadzanych danych, stosowanych zabezpieczeń przed dostępem, sposobu odwzorowywania struktury organizacyjnej opisywanego świata na strukturę bazy.

5. Twórcy WHOIS++, mają do dyspozycji ogrom doświadczeń zebranych przy implementacji X.500. Doświadczenia takie pozwalają stwierdzić jaki jest najbardziej typowy sposób dostępu do danych (na przykład typowe są próby wyszukowania pojedynczych osób z poziomu kraju), jakiego typu narzędzia należy dostarczać twórcom oprogramowania, aby ułatwić im tworzenie nowych produktów w krótkim czasie, jakie są najbardziej podstawowe trudności w funkcjonowaniu takiego rozproszonego systemu itp. Trzeba podkreślić przy tym, że prace nad tworzeniem WHOIS++ prowadzone są przy współudziale osób zajmujących się X.500.

6. X.500 (podobnie jak X.400) od początku tworzone było z myślą o świecie komercyjnym, a nie akademickim. Firmy komercyjne mają zupełnie inne podejście do usług sieciowych, wymagają standardów, gwarancji, zabezpieczeń. Usunięcie takich ograniczeń znacznie ułatwia szybkie tworzenie produktów, ale znacznie zmniejsza ich potencjalny zasięg.

Grupy zaangażowane w prace związane z X.500 zdają sobie sprawę z faktu, że technologia ta, mimo że rozwijała się w sposób ciągły, nie nadążała za lawinowym wzrostem Internetu. W konsekwencji powstało szereg produktów konkurencyjnych stanowiących podbudowę dla *directory service*, abstrahujących od protokołów CCITT/OSI, często bazujących na kilku podstawowych technologiach w celu dostarczenia docelowej usługi katalogowej. Główne powody stosunkowo małej popularności X.500 i jego relatywnie wolnego rozwoju, to skomplikowana technologia, niska efektywność implementacji dostępnych nieodpłatnie, trudności instalacyjne, konfiguracyjne i eksploatacyjne, a także problemy związane z prywatnością danych umieszczanych w bazie X.500. Równie istotną przyczyną wydaje się być dominowanie spraw dotyczących protokołów i ignorowanie przez długi czas efektu docelowego, któremu X.500 ma służyć — dostarczenia niezawodnej usługi katalogowej.

Z drugiej strony, X.500 jest jedyną spójną, jednolitą, wielopłaszczyznową technologią oferowaną dla potrzeb *directory service* i jako taka, szczególnie w swoim nowym standardzie i po uwzględnieniu dotychczasowych doświadczeń eksploatacji pilotowej, wydaje się być znakomitą podstawą do tworzenia uniwersalnej usługi, dostępnej w różnorodnym środowisku sieciowym. Wszystkie pozostałe produkty X.500 zostały rozwinięte *ad hoc*, jako odzew na potrzebę szybkiego dostarczenia docelowej usługi.

Eksploatacja X.500 wskazuje, że jednym z podstawowych wymogów stawianym bazie adresowej jest istnienie możliwości szybkiego wyszukiwania osób poprzez podanie nazwiska, bez dokładnego określenia organizacji. Tego typu zapytania, przy obecnej infrastrukturze rozproszonych serwerów X.500 wymagają przeglądania wielu poddrzew informacji, co jest bardzo nieefektywne. W celu zwiększenia funkcjonalności X.500 zamierza się wprowadzić koncepcję serwerów indeksujących, które będą pełnić podobną rolę jak *archie* dla usługi FTP, czy *Veronica* dla przestrzeni informacyjnej *gophera*. Serwery takie będą gromadziły nazwy haseł określonych DSA, mogą to być oczywiście hasła dotyczące obiektów umiejscowionych w różnych, odseparowanych od siebie miejscach drzewa danych X.500. Przewiduje się, że konieczne będą pewne modyfikacje w sposobie przechowywania informacji o odwołaniach do poszczególnych obszarów, tak, by można określić zakres przeszukiwania. Indeksowe DSA mają istnieć w ramach drzewa DIT, ale nie będą jawnie widoczne. Szczegółowo proponowaną koncepcję omówiono w [13].

Konieczność wprowadzenia indeksowych DSA jest niezaprzeczalna. Jednocześnie narzuca się pytanie dlaczego dopiero teraz. Dla WHOIS++ technologia serwerów indeksowych była fundamentem samego projektu. Aby zrozumieć przyczyny takiej sytuacji należy uświadomić sobie, że w standardzie '88 nie zdefiniowano zasad replikacji. Przybliżony protokół tego typu operacji został określony dla potrzeb Internetu w RFC1276 [2], jednak brakuje w nim elementów dotyczących replikacji poddrzew oraz możliwości tzw. stopniowej aktualizacji (*incremental update*), a poza tym nie został on powszechnie zaimplementowany. Standard '93 zawiera definicję operacji replikacji, co rozwiązuje wiele technicznych problemów przy tworzeniu indeksowych DSA.

4.2 Administrowanie

Kilka lat pracy przy rozwoju X.500 pozwoliło na zebranie doświadczeń związanych z obsługą samych danych.

Na początek należy podkreślić, że rozróżnienia wymaga administrowanie samym systemem od administrowania danymi. Oba zadania są niezmiernie ważne, ale dosyć różne w zakresie obowiązków. W początkowej fazie implementowania bazy zadania te są szczególnie blisko związane ze sobą, jako że naturalnym elementem administrowania systemem jest tworzenie narzędzi programowych, a przy przetwarzaniu danych z najróżnorodniejszych źrodeł takiej pracy jest dużo. Po utworzeniu systemu narzędzi i uruchomieniu stabilnego systemu zbierania informacji, do wykonania pozostaje regularne aktualizowanie danych, co jest czynnością stosunkowo mało interesującą. Trzeba zwracać na to uwagę, aby nie zatrudniać do takich zadań osób zbyt wysoko wykwalifikowanych.

Kolejną sprawą jest fakt, że pozornie ilościowa jedynie różnica pomiędzy administrowaniem bazą eksperymentalną i „produkcyjną", jest w istocie różnicą jakościową. To, co w małej bazie jest do wykonania metodami ingerencji w każde hasło, przy bazie dużej wymaga narzędzi. Duża baza przedstawia informacje dotyczące wielu jednostek, którym nie jest obojętnie jak te informacje są przedstawione. Dobrym przykładem takich problemów może być przetwarzanie danych uzyskanych z Ośrodka Przetwarzania Informacji (OPI). Na pozór sprawa powinna być zupełnie prosta, dokonano zrzutu informacji w postaci pośredniej, wystarczy zatem przetworzyć ją do formatu X.500; w praktyce napotkaliśmy na szereg problemów związanych z niekompatybilnościa formatów — nazwy instytucji są zbyt długie, telefony podawane są w luźnym formacie tekstowym, a nie sformalizowanym jak w X.500, długości nazw polskich ulic przekraczają przyjęte przez twórców X.500 ograniczenie. To jedynie kilka z napotkanych problemów, które są bardzo trudne do rozwiązania, jako że wymagałyby w zasadzie ingerencji administratora w pojedyncze hasła, a w pewnych przypadkach nawet konsultacji z tymi, których dane dotyczą.

4.3 Efektywność

W trakcie prac nad uruchamianiem bazy X.500 przeprowadziliśmy nieco badań efektywnościowych. Teoretycznym rozważaniom nad elementami wpływającymi na sprawność rozproszonej bazy danych poświęciliśmy raport [15].

QUIPU, które było badanym przez nas produktem jest dosyć specyficzne, jako że przechowuje całość danych (za wyjątkiem specyficznych atrybutów jak obraz, czy dźwięk) w pamięci operacyjnej komputera. Fakt ten ma bardzo istotny wpływ na sprawność samej bazy — działanie jest bardzo szybkie w sytuacji, gdy baza faktycznie rezyduje w pamięci, z drugiej strony obsługa pamięci wirtualnej może działanie bazy bardzo spowalniać. W tym zakresie obserwuje się dwa efekty:

1. Baza mieszcząca się w całości w pamięci operacyjnej działa szybko, pod warunkiem, że w okresie bezczynności nie zostanie „wymieciona" przez system na dysk. Jeżeli to nastąpi, to pierwszy po przerwie dostęp do bazy będzie opóźniony, następne są już szybkie.

2. Baza nie mieszcząca się w całości w pamięci wymaga obsługi poprzez stronicowanie pamięci i jest nadzwyczaj nieefektywna. Obserwowaliśmy rezultaty, kiedy odszukanie pojedynczego hasła, w ramach jednego serwera, zabierało ok. 90 sekund, powiększenie pamięci na tej samej maszynie obniżyło ten czas do poniżej sekundy.

Z obserwacji tych wynika wniosek, że należy być ostrożnym przy podejmowaniu decyzji o rozpraszaniu danych. Rozproszenie ma dwa negatywne skutki: opóźnienia sieciowe oraz rzadszy dostęp do serwerów (i w konsekwencji częstsze efekty „wymiatania” procesu na dysk), z drugiej strony baza nie może przekraczać rozsądnych wymiarów, tak aby bez kłopotu mieściła się w pamięci operacyjnj komputera.

Nasze doświadczenia wykazały, że przy typowych rozmiarach baz indeksowanie nie wydaje się mieć pierwszorzędnego znaczenia. Wyniki te mogą jednak zostać zweryfikowane po wykonaniu prób opartych o mocno rozbudowane zapytania.

Gdy rozważa się zagadnienia efektywnościowe bazy, z reguły myśli się wyłącznie o funkcjonowaniu samego serwera, tymczasem czasami pozornie słabe efekty mogą być winą samego oprogramowania dostępowego (klienta). Stwierdziliśmy, że pewne interfejsy rozpowszechniane w ramach pakietu ISODE stosują wyjątkowo źle zaprojektowane algorytmy sortowania otrzymanej listy wyników, nie stosują też buforowania otrzymanych raz danych. Zmiana algorytmu sortowania pozwoliła na przyspieszenie działania klienta o ponad 50 razy.

Kolejna grupa problemów związana jest z opisywaną w kolejnej części internacjonalizacją. Stosowanie dodatkowych atrybutów przechowujących poprawnie napisane nazwy wydaje się być na pierwszy rzut oka prostym rozwiązaniem, po chwili zastanowienia okazuje się jednak, że w wyniku przeszukania poddrzewa zwracane są wynikowe nazwy wyróżnione; składnikami tych nazw są oczywiście relatywne nazwy wyróżnione, a nie specjalne atrybuty przechowujące poprawne nazwy. W wyniku tego, dla wyświetlenia całej nazwy wyróżnionej, w poprawnej pisowni, konieczne jest dokonanie operacji czytania dla każdego obiektu występującego w gałęzi prowadzącej do otrzymanego wyniku. Wpływ takiego działania na efektywność może być katastrofalny, zwłaszcza przy długich listach wynikowych.

4.4 Internacjonalizacja

Istotnym problemem przy popularyzacji bazy danych o zasięgu międzynarodowym jest zapewnienie jej uniwersalności. Podstawowe atrybuty opisujące hasła zgromadzone w X.500 muszą być zapisane w taki sposób, by mogły być odczytane przez dowolne interfejsy użytkowe. Oznacza to, w przypadku Polski, że wszystkie nazwy są okrojone z polskich znaków diakrytycznych. Taka prezentacja danych nie może zadowolić polskiego użytkownika, gdyż bardzo często powoduje utratę istotnej informacji.

Model informacyjny X.500 zapewnia rozszerzalność bazy poprzez tworzenie nowych atrybutów, które nie są interpretowane przez zewnętrzne systemy, nie poinformowane o wprowadzeniu nowych identyfikatorów obiektów. Niestety, eksploatowane w ramach polskiego programu pilotowego oprogramowanie QUIPU dopuszcza wyłącznie interpretację znaków tabeli ASCII i Latin-1 (ISO8859-1). Wewnętrznie X.500 stosuje standard telekomunikacyjny T.61 do kodowania znaków dodatkowych. Wbudowane w QUIPU mechanizmy obsługi łańcuchów T.61 i prezentacji znaków Latin-1 są bardzo ubogie i, jak się okazuje, posiadają wiele błędów implementacyjnych.

W ramach grantu KBN autorzy przeprowadzili wstępne prace mające na celu dostosowanie oprogramowania QUIPU oraz struktury baz X.500 do obsługi polskich znaków diakrytycznych. Opracowane zostały zasady niezbędnych rozszerzeń tablic atrybutów i klas obiektów, dzięki temu zapewniona jest możliwość umieszczania polskich nazw jako oddzielnych atrybutów opisujących hasła. Dokonano analizy oprogramowania w celu umiejscowienia modułów odpowiedzialnych za obsługę translacji kodów, a następnie zostały zmodyfikowane odpowiednie funkcje biblioteczne. W ten sposób zrealizowano obsługę znaków z zakresu tabeli Latin-2 (ISO8859-2), czyli właściwe przekodowanie w przypadku, gdy program użytkowy korzystający z DSA zgłosił się jako interfejs interpretujący taki kod (jest to parametr ustawiany konfiguracyjnie). Jednocześnie konieczne były zmiany w ramach samych programów użytkowych takich jak *Pod*, *dish*, *de*. Ten ostatni został przebudowany w dość szerokim zakresie, z myślą dostarczania go jako typowego polskiego interfejsu użytkowego X.500. Rozważaniom na temat problemów związanych z obsługą znaków narodowych w systemach typu X.500 Directory poświęcony jest raport autorów [14].

Sporo pracy wymagało dostosowanie oprogramowania do obsługi przeszukiwania bazy X.500 po podaniu polskiego wzorca danych, gdyż niestety, również w tym zakresie produkt nie działał prawidlowo. Obecnie, poprawione funkcje biblioteczne oraz program obsługi DSA prawidłowo realizują tego typu wyszukania. Należy jednak pamiętać, że w tym celu niezbędna jest eksploatacja zmodyfikowanego oprogramowania serwera QUIPU oraz DUA skompilowanych na bazie poprawionych bibliotek.

Działania dotyczące internacjonalizacji X.500 są prowadzone nadal. Uważamy, że jest to priorytetowe zadanie polskiego programu X.500. Zamierzamy kontynuować pracę nad dostosowaniem różnych DUA do obsługi polskich znaków, jak również prowadzić działania na forum międzynarodowym zmierzające do uwypuklenia problemu stosowania lokalnego nazewnictwa.

Nowy standard '93 przewiduje istnienie tzw. łańcuchów BMP (Base Modular Plan), reprezentujących znaki według standardu ISO 10646. Być może nowe implementacje X.500 uproszczą dzięki temu wprowadzanie lokalnych nazw do bazy danych.

Grupa rozwijająca europejski projekt X.500 rozważa również możliwość pełnej internacjonalizacji poprzez wbudowanie w DSA odpowiednich mechanizmów tłumaczących według odpowiednich słowników. Abstrahując od sensowności takiego rozbudowywania DSA, wydaje się, że wobec nawału prac związanych z nowym standardem perspektywy urzeczywistnienia tego typu planów są znikome. Brakuje niestety odpowiedniego forum forsującego problematykę znaków międzynarodowych w bazach danych, w efekcie administratorzy krajowi są zmuszani do indywidualnych prac, często dublujących już wykonane.

5 Powiązania X.500 z innymi standardami i systemami

W środowisku Internetu trwają dyskusje na temat modelu usługi katalogowej (*Directory Service*). Istnieje grupa przeciwników X.500, która zarzuca standardowi nieefektywność, brak jednoznacznej definicji niektórych elementów protokołu i, co za tym idzie, niemożliwość spójnej implementacji oraz duży ciężar protokołu obarczonego obsługą modelu sieciowego OSI.

Nowy standard X.500 '93 zawiera szereg poprawek i rozszerzeń (patrz część 6), wydaje się że jego pełna implementacja pozwoliłaby uniknąć wiele problemów, z którymi produkty wersji '88 próbują uporać się w różny, nie zawsze wzajemnie kompatybilny sposób. Wiodący producenci oprogramowania X.500: ISODE Consortium, NEXOR, DEC, już przystąpili do prac mających na celu wdrożenie nowego standardu, jednak ze względu na rozległość zmian nie jest możliwa szybka modyfikacja istniejącego oprogramowania.

Tymczasem istnieją grupy, w których trwają prace nad definicją i implementacją uproszczonych protokołów realizujących analogiczną usługę dostępu do baz informacyjnych typu „książka adresowa" (*White Pages*).

5.1 WHOIS++

Jednym z głównych konkurentów jest protokół WHOIS++, rozwijający się na bazie zdefiniowanego w 1982 roku NICNAME/WHOIS ([6]). Patronowana przez Network Information Center (NIC) usługa WHOIS miała na celu dostarczenie w sieci Internet danych o użytkownikach, organizacjach, zasobach sprzętowych i programowych. W pierwotnym zamierzeniu baza ta była pomyślana jako wielodostępna, rezydująca na określonym serwerze i udostępniająca w prostym formacie dane o obiektach zarejestrowanych w NIC. Podstawowa usługa szybko rozszerzyła się i gwałtownie wzrosła liczba niezależnych komputerów oferujących tego typu dane. Model informacyjny protokołu WHOIS ograniczał skalę zastosowania, tymczasem popularność usługi świadczyła o niezbędności jej udoskonalenia i wdrożenia. Spowodowało to rozwój kolejnej wersji, znanej jako WHOIS++, o rozbudowanym modelu danych, wzbogaconym mechanizmie formułowania zapytań i przeszukiwania.

Architektura usługi katalogowej WHOIS++ jest rozdzielona pomiędzy dwa komponenty: serwer poziomu podstawowego oraz indeksujący. Standard WHOIS++ opisują dokumenty Internet–Draft [7] i [8]. W praktyce jeden serwer fizyczny może spełniać obie funkcje, czyli gromadzić dane według ustalonego schematu oraz utrzymywać indeks, zawierający wskazania do innych serwerów.

Stosowana zasada indeksowania polega na tworzeniu na podstawie informacji zawartej w ramach serwerów, odwzorowania postaci tzw. *centroid*, będących hasłami, które dla każdego typu atrybutu gromadzą jego wartości. Dane te są zarządzane przez serwery indeksujące, zbierające „centroidy” własne oraz wybranych serwerów indeksujących. WHOIS++ uwzględnia również rozproszone zarządzanie bazą danych.

Autorzy protokołu WHOIS++ twierdzą, że w wielu przypadkach jego zwięzłość i prostota może zadecydować o wyborze tej technologii w celu implementacji *directory services*. Podkreśla się efektywność wybranej metody indeksacji, zarzucając standardowi X.500 brak mechanizmu pozwalającego w sposób optymalny przekazywać zapytania do kolejnych serwerów.

5.2 SOLO

SOLO (Simple Object Look-up Protocol) to kolejna próba specyfikacji usługi zwanej *directory service* ([9]). Protokół ten jest rozwijany we Francji (INRIA), jego autorzy bazują na doświadczeniach związanych z X.500, wykorzystują zainicjowane w ramach X.500 „przyjazne” nazewnictwo obiektów (*user friendly naming*) oraz koncepcje indeksowania (*centroids*) stosowaną w WHOIS++. Podstawowym motywem przy defincji tego standardu było powstanie systemu dostarczającego z jednej strony mechanizmy prostego dostępu do serwerów pracujących według innych protokołów — WHOIS czy X.500, a jednocześnie dającego możliwość tworzenia oprogramowania pośredniczącego pomiędzy tymi protokołami (typu *gateway*).

SOLO to prosty protokół tekstowy, pracujący na platformie połączeń TCP/IP, który opiera się na dwóch podstawowych operacjach:

- przeszukiwania — w celu odzyskania informacji o określonym obiekcie,
- transferu strefy — operacji wykonywanej dla aktualizacji indeksów w ramach serwera; indeksowanie odbywa się analogicznie jak w protokole WHOIS++ poprzez tworzenie tzw. *centroid*, czyli jednego ogromnego hasła (*entry*), zawierającego wartości atrybutów dla wszystkich indeksowanych typów atrybutów opisujących obiekty.

5.3 X.500 a inne systemy informacyjne

Zasoby sieci Internet oferowane są poprzez różnego typu systemy realizujące funkcje naprowadzania i udostępniana informacji na bazie wielopoziomowych menu. Jednym z nich jest opracowany w 1991 w University of Minnesota *gopher*. Obecnie wszystko wskazuje na to, że następcą *gophera* zostanie system *World Wide Web — WWW*, który spowodował prawdziwą rewolucję w dziedzinie prezentacji danych w sieci Internet.

Baza X.500 Directory jest dostępna z tych popularnych systemów dzięki istnieniu specjalnych programów translujących odpowiednie protokoły (oprogramowanie typu *gateway*). Na ogół możliwości te są realizowane na bazie protokołów LDAP czy SOLO jako pośredniczących w kontakcie z X.500, co wskazuje, że twórcy programów użytkowych dla X.500 preferują specyfikacje mniej rozbudowane.

Bardzo istotnym czynnikiem, jakie wniósł rozwój WWW jest jednorodne nazewnictwo zasobów komputerowych za pomocą tzw. Universal Resource Locators (URL). Nazwa taka zawiera rodzaj i lokalizację zasobu, łącznie z formą dostępu do niego.

X.500 Directory uwzględnia obecnie możliwość podawania umiejscowienia obiektu za pomocą URL, zasady określa opublikowany dokument serii serii Internet Draft [10].

Przy okazji warto wspomnieć o funkcjonowaniu wyspecjalizowanych systemów katalogowych, np. skupiających dane o osobach określonej specjalności. Wydaje się, że dążenie do utrzymywania jednej tylko globalnej dazy danych, która udostępniałaby określone podzbiory danych w formie projekcji, jest nierealne. Baza utrzymywana w formie rozproszonej i obejmująca swoim zasięgiem ogromne ilości informacji, nie może być tak jednorodna oraz dawać gwarancję, że przedstawia obraz pełny i bez przekłamań. Nie oznacza to bynajmniej, że nie należy myśleć o stosowaniu X.500 do usług typu *Yellow Pages*, twierdzimy tylko, że X.500 nie będzie w stanie wyprzeć niewielkich i silnie specjalizowanych baz danych.

5.4 Wykorzystanie X.500 dla potrzeb poczty elektronicznej

Głównym motywem rozwoju X.500 była potrzeba odwzorowania skomplikowanych adresów poczty elektronicznej X.400 na identyfikatory użytkowników. W miarę rozwoju, zakres zastosowania X.500 rozbudował się i często technologia ta jest stosowana jako sposób reprezentacji książki telefonicznej, czy adresowej.

Już obecnie istnieją produkty, które integrują usługę X.500 z pocztą elektroniczną, dostarczając użytkownikom Internetu wygodną metodę wyszukiwania adresów e-mail z baz X.500 Directory. Programy takie pracują na różnych platformach systemowych (Unix, DOS, Macintosh OS). Rosnąca popularyzacja poczty elektronicznej, która staje się obecnie podstawową formą wymiany informacji pociąga za sobą konieczność szerszego rozpowszechniania X.500 jako infrastruktury e-mail.

Programy pilotowe poczty X.400, działające w wielu środowiskach akademickich Europy (Anglia, Holandia, Niemcy) wykorzystują X.500 jako miejsce przechowywania informacji o sposobie przekazywania komunikatów (*routing*) pomiędzy kolejnymi MTA (*Message Transfer Agent*), w celu dostarczenia poczty od adresata do odbiorcy, czy do określenia możliwości programów użytkowych (*User Agent*), co jest szczególnie istotne w przypadku poczty multimedialnej (MIME).

X.500 może być również stosowane do przechowywania adresów członków list dystrybucyjnych, co dzięki rozproszonemu zarządzaniu X.500 pozwala na zmianę adresu e-mail osoby bez konieczności informowania administratora listy.

Obecnie rozwija się wykorzystanie X.500 w poczcie prywatnej — PEM (Privacy Enhanced Mail). PEM stosuje machanizm kluczy publicznych do bezpiecznej wymiany komunikatów, wysyłana poczta może zostać zaszyfrowana kluczem publicznym odbiorcy, który jest jedyną osobą mającą prawo do odkodowania informacji poprzez podanie klucza prywatnego. Używanie PEM wymaga zapewnienia dostępu do kluczy publicznych wszystkich potencjalnych adresatów. X.500 pozwala przechowywać tego typu dane w ramach swoich rozproszonych baz danych. Należy podkreślić, że architektura zarządzania kluczami szyfrującymi stosowana w PEM ([4], [5]) bazuje na koncepcji certyfikatów kluczy publicznych zdefiniowanej w serii X.509, będącej zaleceniami CCITT dotyczącymi metod poświadczania w ramach X.500 Directory. Ponadto, certyfikaty wykorzystują określoną w X.500 postać reprezentacji nazw (*Distinguished Names*). Organizacje posiadające uprawnienia do przydzielania kluczy publicznych — *Certification Authorities*, mają w ramach drzewa X.500 przydzielone odpowiednie hasła.

Analiza nowej wersji standardu X.500 pozwala odeprzeć wiele zarzutów dotyczących możliwości oferowanych w ramach samego protokołu. Nie sposób jednocześnie zaprzeczyć, że X.500 jest protokołem rozległym, wymagającym ogromnego wysiłku implementacyjnego. Jednak w przypadku konstruowania aplikacji sieciowych, które mają zadawalać szeroką rzeszę użytkowników i spełniać różnorodne wymagania, konieczny staje sie wybór pomiędzy niezbędnymi nakładami pracy a oczekiwanymi efektami, jakie ma dać gotowy system. Najistotniejszym celem powinno być powstanie systemu, na bazie którego będzie można w przyszłości szybko i tanio budować oprogramowanie typu użytkowego, „klienckiego".

6 Rozwój standardu (X.500 '93)

Nowa wersja standardu została ogromnie rozbudowana w stosunku do swojej pierwszej wersji. Autorzy starali się usunąć zauważone niejasności, jak również dodać elementy, których do tej pory ewidentnie brakowało. Najbardziej odczuwalny był brak:

- replikacji danych,
- kontrolowania dostępu do danych,
- rozdziału atrybutów na użytkowe i operacyjne, tj. przechowyjących informacje potrzebne potencjalnemu odbiorcy i te potrzebne dla poprawnego funkcjonowania bazy,
- wprowadzenie atrybutów zbiorowych, wspólnych dla całej grupy obiektów.

Dwa pierwsze punkty zamiplementowano w QUIPU jako rozszerzenia standardu '88, uważając, że są niezbędne do uruchomienia sprawnie działającej usługi. Standard '93 podchodzi do tych spraw inaczej niż określono to w rozszerzeniach stosowanych w QUIPU, co pociąga za sobą niekompatybilność produktów.

Odnośnie replikacji administratorzy będą mieli znacznie szersze możliwości niż dawało im QUIPU, będą mogli replikować całe wybrane fragmenty drzewa, a nie jak do tej pory tylko pojedynczy poziom, replikacji będa mogły podlegać tylko wybrane grupy atrybutów, wywołanie protokołu replikacji będzie mogło następować z inicjatywy dowolnej ze stron. W związku z tym konieczne było wzbogacenie protokołu zapytań o opcje sterujące tym, czy pytający zadowala się informacją zreplikowaną, być może niekompletną, czy też niezbędny jest oryginał.

Kontrolowanie dostępu będzie zapewniało duży stopień bezpieczeństwa (standardowo stosowane obecnie w QUIPU zabezpieczenia, są proste do złamania), rozbudowany jest także mechanizm zabezpieczeń dając wielostopniowy system ochrony (np. ochrona przed wyświetlaniem listy, przeszukiwaniem, wyświetlaniem wartości, informowaniem o istnieniu itp.).

Rozdział atrybutów będzie miał pozytywny wpływ na użytkowanie bazy, kiedy osoba pobierająca informację nie będzie już dostawała całkowicie zbędnych atrybutów administracyjnych.

Wprowadzenie atrybutów grupowych stanowi konieczne uzupełnienie poprzedniego standardu. QUIPU stosowało atrybuty dziedziczone, atrybuty zbiorowe będą rozszerzały ich funkcjonalność.

Różnice między obiema wersjami standardu są bardzo znaczne, ale szczególowe ich wyjaśnienie wykracza znacznie poza zakres niniejszego artykułu. Zainteresowanych czytelników odsyłamy do opracowania [11].

7 Literatura uzupełniająca

Poniżej zamieszczamy wykaz pozycji, których lekturę zalecamy czytelnikowi zainteresownemu szczegółowo problematyką X.500.

- C.J. Robbins, S.E. Kille (1992) *The ISO Development Environment: User's Manual, Volume 5: QUIPU*
- Marshall T. Rose (1992) *The Little Black Book: Mail Bounding with OSI Directory Services*
- D. Chadwick (1994) *Understanding X.500 The Directory*

Bibliografia

[1] Data Communication Networks: Directory, Recommendations X500-X.521, CCITT, Fascile VIII.8 of Blue Book.

[2] S. E. Hardcastle-Kille (1991) *Replication and distributed operation extentions to provide an Internet Directory using X.500, Request for Comments RFC1276*
URL=<ftp://ds.internic.net/rfc/rfc1276.txt>

[3] A. Getchell, *A Revised Catalog of Available X.500 Implementations*, Request for Comments RFC1632
URL=<ftp://ds.internic.net/rfc/rfc1632.txt>

[4] J. Linn (1993) *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures* Request for Comments RFC1421
URL=<ftp://ds.internic.net/rfc/rfc1421.txt>

[5] S. Kent (1993) *Privacy Enhancement for Internet Electronic Mail: Part I: Certificate-Based Key Management* Request for Comments RFC1422
URL=<ftp://ds.internic.net/rfc/rfc1422.txt>

[6] E. Finler, K. Harrenstien, M. Stahl (1985) *NICNAME/WHOIS*, Request for Comments RFC954
URL=<ftp://ds.internic.net/rfc/rfc954.txt>

[7] P. Deutsch, R. Schoultz, P. Faltstrom, C. Weider (1995) *Architecture of the WHOIS++ service*, Internet Draft
URL=<ftp://ds.internic.net/internet-drafts/drafts-ietf-wnils-whois-arch-02.txt>

[8] C. Weider, J. Fullton, S. Spero (1994) *Architecture of the WHOIS++ Index Service*, Internet Draft
URL=<ftp://ds.internic.net/internet-drafts/drafts-ietf-wnils-whois-03.txt>

[9] C. Huitema, P-A. Pays, A. Zahm, A. Woermann (1994) *Simple Object Look-up protocol (SOLO)*, Internet Draft
URL=<ftp://ds.internic.net/internet-drafts/drafts-huitema-solo-01.txt>

[10] Mark Smith (1995) *Definition of an X.500 Attribute Type and Object Class to Hold Uniform Resource Identifiers (URIs)* Internet Draft
URL=<ftp://ds.internic.net/internet-drafts/draft-ietf-asid-x500-url-01.txt>

[11] A. Waugh (1994) *X.500 and the 1993 Standard*

[12] A. Waugh (1994) *Where are the Network Applications?*, Australian Networkshop '93, Melbourne
URL=<ftp://ftp.unimelb.edu.au/pub/networkshop93/infores/waugh.txt>

[13] P. Barker (1995) *X.500 Index DSAs*

[14] M. Górecka, T. Wolniewicz (1994) *Ocena efektywności rozproszonej bazy danych na podstawie X.500 Directory*, Raport NASK

[15] M. Górecka, T. Wolniewicz (1994) *Stosowanie znaków diakrytycznych w systemach baz danych X.500*, Raport NASK