INFORMACYJNO-ADRESOWA BAZA DANYCH WEDŁUG STANDARDU X.500 W POLSKIM ŚRODOWISKU AKADEMICKO-NAUKOWYM

Maja Górecka *Maja.Gorecka@cc.uni.torun.pl*

Tomasz Wolniewicz *twoln@hpc.uni.torun.pl*

Ogólnouczelniany Ośrodek Obliczeniowy, Uniwersytet Mikołaja Kopernika
Chopina 12/18, 87-100 Toruń

1. Wstęp

Referat prezentuje usługę X.500, funkcjonującą w polskim Internecie od ponad czterech lat, oferującą dane adresowe i informacyjne o polskich uczelniach i jej pracownikach. Podajemy w skrócie podstawowy opis międzynarodowych rekomendacji standardu X.500 (ISO/IEC Directory Standard / CCITT X.500 Recommendations), na których opiera się praca systemu. Omawiamy rozwój serwisu X.500 w Polsce, koordynowany przez nas z ramienia NASK od 1992 roku oraz przedstawiamy prowadzone prace badawczo-rozwojowe w zakresie X.500.

2. Standard X.500 Directory

Standard X.500 jest zdefiniowany jako seria rekomendacji, które powstały w efekcie równoległych prac CCITT (Consultative Committee for International Telegraph and Telephone, obecnie ITU-T) oraz ISO (International Standards Organization). Pierwsza wersja standardu określana jest jako X.500'84, kolejne to '88 oraz '93. Podstawową przyczyną powstania X.500 była potrzeba istnienia rozproszonej bazy danych, gromadzącej dane wspomagające procesy komunikowania się procesów komputerowych i ich użytkowników. Początkowo myślano o wykorzystywaniu przez systemy OSI, głównie przez system pocztowy X.400 MHS, do wprowadzania adresów e-mail, list dystrybucyjnych czy wyszukiwania danych dotyczących udostępnianych w środowisku sieciowym aplikacji użytkowych. Docelowo, zakres zastosowań uległ znacznemu rozszerzeniu, bazę X.500 wykorzystuje się do gromadzenia informacji o adresach e-mail (Internetowych oraz X.400) oraz innych danych opisujących instytucje i osoby, jak adresy pocztowe, telefony, faxy, tytuły naukowe, zainteresowania zawodowe.

Model funkcjonalny i administracyjny X.500 definiuje sposób rozproszenia zasobów X.500, model informacyjny opisuje logiczną strukturę bazy danych, zasady pracy specyfikują rodzaje operacji dokonywanych na zasobach i przebieg ich realizacji, natomiast model bezpieczeństwa przedstawia sposoby ochrony danych w X.500 Directory i kontrolowania dostępu do nich.

W 1995 roku sfinalizowano prace nad rozszerzeniami protokołu X.500. Najistotniejsze elementy nowego standardu, opublikowanego jako X.500'93, dotyczą replikacji danych, kontroli dostępu do zasobów, zarządzania strukturą bazy (*schema*) oraz informacją o rozproszonym systemie (*knowledge referece*). W dalszej cześci opracowania będziemy powracać do tematu nowej edycji standardu.

Podstawowe terminy stosowane w ramach X.500 to:

- **Directory** — zbiór informacji, zwany również DIB (*Directory Information Base*) — baza informacyjna X.500,

- **DSA** (*Directory System Agent*) — oznacza aplikację pełniącą funkcję serwera, który obsługuje wybrany obszar administracyjny, np. instytucję,
- **DUA** (*Directory User Agent*) — oznacza aplikację reprezentującą użytkownika korzystającego z zasobów X.500.

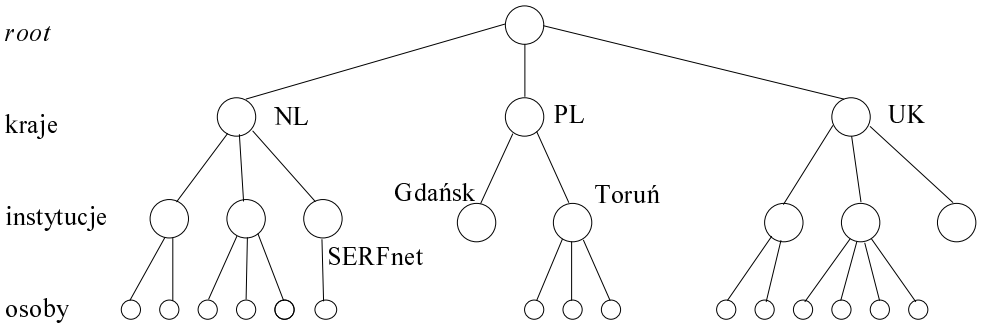
Model informacyjny

Zasoby informacyjne X.500 to nie tylko dane użytkowe, również elementy operacyjno-administracyjne, niezbędne do synchronizacji pracy rozproszonego systemu. Serwer DSA jest w rzeczywistości bazą danych przechowującą informacje w formacie standardu X.500 i mającą możliwość wymiany danych z innymi serwerami.

Podstawowe wymagania stawiane systemowi X.500 z punktu widzenia jego funkcjonalności, takie jak:

1. znaczne rozproszenie zasobów,
2. konieczność zarządzania bardzo rozległą bazą informacyjną,
3. zapewnienie jednoznacznego nazewnictwa,
4. łatwość wyszukiwania danych

uniemożliwiają stosowanie płaskiej struktury zasobów. Wykorzystano powszechne relacje pomiędzy hasłami (np. osoba pracuje w oddziale należącym do instytucji rangi krajowej) i zdefiniowano bazę X.500 jako strukturę hierarchiczną, zwaną drzewem informacyjnym (DIT — *Directory Information Tree*). DIT to wirtualna hierarchiczna struktura danych, składająca się z korzenia (*root*), pod którym umieszczone są kraje i organizacje międzynarodowe, poniżej definiuje się instytucje, którym z kolei podporządkowane są jednostki organizacyjne. Przedstawiony schemat obrazuje DIT reprezentujący globalne zasoby X.500.



Każdy serwer X.500, zwany DSA zarządza częścią zasobów globalnych oraz potrafi, dzięki hierarchicznej strukturze zasobów, wyszukać DSA utrzymujące dane z interesującego użytkownika zakresu. X.500 dostarcza mechanizmy pozwalające przechowywać lokalnie dane informacyjno-adresowe oraz umożliwiające zarządzanie nimi i zapewnianie ich aktualność. Lokalnie dostępny system X.500 w przypadku otrzymania zapytania o dane spoza obejmowanego przez niego obszaru, przekazuje zlecenie kolejnym systemom i odbiera wynik, fakt wykonywania zdalnych operacji jest ukryty przed użytkownikiem, dla którego X.500 ma postać rozległej bazy danych obejmującej swym zakresem cały świat.

Informacja jest gromadzona w X.500 w postaci haseł (*entries*), oznaczających nazwane zestawy informacji opisujące obiekty świata rzeczywistego. Hasło należy do wybranej klasy obiektów, definiującej i klasyfikującej obiekt za pomocą zbioru atrybutów. Każdy atrybut posiada typ i wartość (jedną lub wiele). Rodzaj atrybutów zależy od tego, do jakiej klasy obiektów należy hasło. Np. klasa obiektów *osoba* (*person*) dopuszcza typy atrybutów

commonName, *telephoneNumber*, *mail*, natomiast klasa *instytucja* (*organisation*) stosuje typy: *organisationName*, *BusinessCategory*.

Co najmniej jedna wartość atrybutu jest wyróżniona i stosowana do nazwania hasła, np. hasło reprezentujące osobę używa jako atrybutu wyróżnionego common name. Nazwa hasła musi być unikalna na danym poziomie drzewa informacji. Pełna nazwa hasła, zwana DN (*Distinguished Name*) jest sekwencją nazw począwszy od poziomu root, na bieżącym haśle kończąc. Standard X.500 dopuszcza również wprowadzanie nazw aliasowych, wówczas atrybut aliasedEntryName wskazuje właściwy obiekt.

Model Bazy

W ramach tego modelu standard definiuje:

– model funkcjonalny – określa zasady działania bazy, sposób dostępu do zasobów przez użytkowników, komunikacji między klientami a serwerem oraz między serwerami, definiuje metody obsługi zleceń zdalnych,

– model organizacyjny – określa zasady zarządzania bazą podzieloną na tzw. domeny zarządzania (*Directory Management Domain* — DMD); domena administracyjna składa się z minimum jednego DSA, zarządzającego poddrzewem danych w X.500, DMD może udostępniać interfejsy DUA.

Protokoły komunikacji

Sposób realizacji zleceń związanych z przekazywaniem informacji pomiędzy serwerami DSA oraz między DSA a użytkownikiem (DUA) określają odpowiednio protokoły DSP (*Directory System Protocol*) oraz DAP (*Directory Access Protocol*), definiujące dopuszczalne operacje zdalne oraz metody komunikowania. Każdy serwer DSA musi znać sposób dostępu do DSA zarządzającego kontekstem bezpośrednio powyżej (*superior*), jak również do serwerów administrujących kontekstami bezpośrednio poniższymi (*subordinate*). Taka organizacja umożliwia dostęp do wybranego fragmentu poddrzewa danych za pomocą jednej z dwóch metod:

– odesłania (*referral*) – polega na przekazaniu wskazania kolejnego serwera, który prawdopodobnie może odpowiedzieć na zlecenie,

– tworzenia łańcuchów (*chaining*) – wykonania połączenia do kolejnego DSA w imieniu pytającego i pośredniczenie w odbiorze wyniku.

Model bezpieczeństwa

Określa metody poświadczania tożsamości przy stosowaniu usługi X.500 oraz autoryzacji dostępu do danych (*authentication* i *authorization*). Zasoby bazy X.500 mogą mieć nadane przez administratora prawa dostępu, ddotyczy to poddrzewa informacji, albo określonych atrybutów (np. numer telefonu).

3. Oprogramowanie implementujące standard X.500

Rozwój projektu X.500 był możliwy dzięki pakietowi Isode, zawierającemu moduły implementujące warstwy OSI, a w warstwie aplikacji m.in. FTAM (*File Transfer Access Method*), VT (*Virtual Terminal*) oraz standard X.500 – ta część pakietu została nazwana QUIPU. Oprogramowanie QUIPU jest ogólnodostępne w ramach pakietu Isode, ale nie jest ono rozwijane od 1992 (ostatnia edycja to Isode-8.0). W oparciu o Isode tworzone były między innymi produkty oferowane przez Isode Consortium oraz firmę Nexor (Wielka Brytania). Isode Consortium do jesieni ubiegłego roku udzielało bezpłatnych licencji wszystkim jednostkom aka-

demicko-naukowym zgłaszającym się z chęcią wykorzystania oprogramownia (zwanego IC). Obecnie Isode Consortium przekształciło się w firmę Isode i umożliwia uzyskanie praw do użytkowania oprogramowania po opłaceniu subskrypcji rocznej. Inne firmy oferują komercyjne oprogramowanie implementujące X.500, na rynku dostępne są m.in. produkty: DEC X.500, DIR.X (Simens Nixdorf), HP X.500, XT-QUIPU Nexora, ICL, czy ISOCOR.

Najnowsze wersje oprogramowania implementują większość nowych cech standardu X.500'93, co jest istotnym przełomem w funkcjonowaniu tej usługi.

4. Udział Polski w światowej usłudze X.500

Rozwój X.500 w Europie zainicjowała działalność University of London Computer Centre, który w ramach projektu Paradise od 1990 roku koordynował pracę serwerów uruchamianych początkowo głównie w jednostkach akademicko-naukowych. Większość serwerów działała wówczas w oparciu o opisywane w poprzednim rozdziale oprogramowanie QUIPU. Również kraje spoza Europy, przede wszystkim Stany Zjednoczone i Australia rozpoczęły swoją działalność w dziedzinie X.500. W 1994 roku projekt Paradise został przejęty przez organizację europejską DANTE i obecnie funkcjonuje pod nazwą NameFLOW-Paradise. Uczestniczy w nim ponad 50 krajów.

Polska zarejestrowała krajowy serwer X.500 w czerwcu 1992 roku, zarządza nim Uniwersytet Mikołaja Kopernika w Toruniu. Równocześnie uruchomiono serwer obsługujący Uniwersytet. Powstał projekt rozwoju X.500 w Polsce, który pod koniec 1992 został przyjęty przez NASK i od tego czasu koordynujemy ogólnopolską usługę X.500.

Początkowo polski projekt X.500, zresztą podobnie jak w wielu innych krajach, rozwijał się żywiołowo, ośrodki zainteresowane świadczeniem usługi uruchomiły własne serwery, Toruń administrując serwerem krajowym koordynował prace. Niestety, samo wystartowanie serwera nie wystarcza, należy załadować bazę danych i utrzymywać ją w aktualnym stanie, a to zadanie wymaga żmudnej pracy. Istotnym przełomem był rok 1994, kiedy UMK w Toruniu otrzymał grant na aktualizację bazy X.500. Fundusze zostały rozdysponowane między ośrodki uczestniczące w projekcie, reprezentujące Warszawę, Wrocław, Poznań, Kraków i Toruń. UMK poza administrowaniem danymi swojej uczelni było odpowiedzialne za utrzymywanie danych tych wszystkich jednostek akademickich, którymi nie opiekują się partnerzy regionalni. Znacznie poprawiła się jakość oferowanej informacji. Kolejny grant KBN na X.500, przyznany w 1996, umożliwił dołączenie nowych miast do projektu, usługę uruchomiono w Gdańsku, Łodzi, Szczecinie, ośrodki aktywne przejęły z serwera krajowego dane uczelni w swoich regionach i zobowiązały się do ich aktualizacji.

UMK zarządzając polskim projektem prowadzi działalność popularyzatorską w zakresie X.500. Nie pozostaje ona bez odzewu. Zgłaszają się reprezentanci kolejnych uczelni, zachęceni do wystartowania usługi, kolejne serwery pojawiają się również w takich miastach jak Wrocław, czy Gdańsk i udostępniają wysokiej jakości dane o swoich uczelniach.

Tymczasem na arenie międzynarodowej zaawansowane są prace nad konkurencyjnymi protokołami posiadającymi funkcjonalność systemu katalogowego, czy bazy informacyjnej. Aktualnie najintennsywniej rozwija się LDAP (*Lightweight Directory Access Protocol*), który z prostego protokołu klient-serwer, zapewniającego dostęp do X.500 urósł do roli standardu Internetu, definiującego sposób dostępu do baz typu katalogowego (*Directory Systems*). Ponad 40 firm, m.in. Microsoft, Novell, Netscape, IBM ma w swoich produktach wbudowaną implementację LDAP. Obecnie serwery katalogowe nie muszą być zgodne z X.500, istnieją samodzielne serwery jak SLDAP (rozwijany przez University of Michigan), czy NDS (Novell). Systemy LDAP współpracują z bazami w standardzie X.500.

5. Prace adaptacyjno-rozwojowe w zakresie X.500

Zespół UMK jako koordynator projektu X.500 systematycznie uczestniczy w międzynarodowych spotkaniach krajowych administratorów DSA i śledzi kierunki rozwoju światowego przedsięwzięcia. Ponadto od początku prowadzone są prace nad oprogramowaniem X.500.

5.1. Dostosowanie bazy X.500 do potrzeb polskich użytkowników

Baza X.500 w polskim środowisku musi umożliwiać wprowadzanie prawidłowych polskich nazw, niezbędne jest również dysponowanie technikami wyszukiwania polskich danych oraz właściwego prezentowania wyników. Podstawowe oprogramowanie umożliwia wyłącznie gromadzenie danych z uwzględnieniem polskich znaków diakrytycznych (QUIPU stosuje do tego celu standard telekomunikacyjny T.61). Nie są natomiast zaimplementowane mechanizmy wyprowadzania danych z uwzględnieniem strony kodowej stosowanej w Polsce — Latin-2. Prace w zakresie dostosowania pakietu QUIPU w tym zakresie są prowadzone od kilku lat. W pierwszym etapie zaprojektowano strukturę informacyjną polskiej bazy X.500. Wykorzystano możliwość lokalnego rozszerzania typu informacji przechowywanej w zasobach X.500, poprzez definiowanie nowych klas obiektów oraz nowych atrybutów. Taka rozbudowa pozwala umieścić informacje w języku polskim w „polskich" (lokalnych) atrybutach, które nie są widoczne przez użytkowników spoza kraju. Wszystkie serwery pracujące w Polsce używają nowe, zawierające polskie dodatki tablice klas obiektów i atrybutów. Ponadto wykonane zostały modyfikacje bibliotek Isode, aby realizować przekodowania zgodne ze stroną Latin-2. Kolejną, niebagatelną sprawą był przygotowanie interfejsu do bazy X.500 dla polskich użytkowników. Chodziło tu o zaimplementowanie w programie następujących funkcji:

- pobierania informacji umieszczonej w ramach rozszerzonych klas obiektów,
- prawidłowe wypisywanie wyników,
- posługiwanie się polskimi komunikatami.

Ponieważ w ostatnim czasie dominuje dostęp do zasobów informacyjnych poprzez przeglądarki WWW zdecydowaliśmy się dostosować do polskich potrzeb program `web500gw`, napisany przez Franka Richtera z Technical University w Chemnitz. Gateway X.500-WWW w polskiej edycji został rozbudowany o możliwości wyszukiwania według podanego adresu e-mail, pobrania klucza publicznego oraz pośredniej modyfikacji swoich zasobów poprzez wysłanie do administratora formularza zawierającego poprawki. Prace nad programem ciągle trwają, plany związane z jego rozwojem w celu zwiększenia funkcjonalności są rozległe.

5.2. Zastosowanie bazy X.500

Model informacyjny X.500 sprawia, że bazę tą cechuje elastyczność, może przechowywać obiekty różnego typu, dopuszcza się także rozszerzanie definicji obiektu poprzez dodanie nowych opisów (atrybutów). Oznacza to, że zastosowania tej bazy mogą być różnorodne. W wielu instytucjach w Stanach Zjednoczonych w oparciu o ten standard tworzone są bazy pracownicze, obsługujące m.in. autoryzację dostępu do pomieszczeń czy komputerów. Uniwersytet Mikołaja Kopernika w Toruniu pracuje obecnie nad przystosowaniem bazy X.500 do funkcji centralnego systemu informacyjnego, aktualizowanego przez jednostki uczelniane i dającego możliwość generowania na podstawie zasobów różnego typu wyciągów drukowanych. Poza tym od 1996 pracujemy nad wykorzystaniem zasobów X.500 do przechowywania kluczy publicznych PGP i PEM. Narzędzia niezbędne do funkcjonowania usługi są gotowe, pozostaje formalne zatwierdzenie struktur administracyjnych odpowiedzialnych za poświadczanie kluczy.

5.3. Prace związane z nowym standardem

Pojawienie się nowego standardu X.500 oraz jego implementacji zapowiada w najbliższej przyszłości istotne zmiany w światowym projekcie X.500, przede wszystkim dlatego, że X.500'93 definiuje odmienny model zwany *knowledge reference*, związany ze sposobem utrzymywania w bazie X.500 danych dotyczących serwerów DSA. W maju 1997 odbędzie się druga faza testów pracy serwerów X.500'93. Testy te są prowadzane przez DANTE. Do udziału w nich niezbędne jest posiadanie oprogramowania IC w wersji 3.0, Uniwersytet w Toruniu w ubiegłym roku opłacił subskrypcje (oferowaną z 50% bonifikatą) i dzięki temu wszedł w posiadanie praw do dostępu do najnowszego oprogramowania przez cały bieżący rok. Możemy więc uczestniczyć w przedsięwzięciach międzynarodowych, ale przede wszystki poznajemy nowy pakiet i prowadzimy prace eksperymentalne.

6. Zasoby informacyjne polskiej usługi X.500

Ogólnopolska strona WWW projektu X.500:

http://ocelot.uni.torun.pl

Archiwum FTP:

ftp://ocelot.uni.torun.pl

Kontakt w sprawie uruchomienia serwera X.500:

x500@cc.uni.torun.pl

Adresy programów ogólnego dostępu oferowanych przez środowiska prowadzące serwis X.500 w Polsce:

URL	Region
rlogin://dish@x500.uni.torun.pl rlogin://de@x500.uni.torun.pl http://x500.uni.torun.pl:8888	Toruń
rlogin://de@x500.pwr.wroc.pl rlogin://sd@x500.pwr.wroc.pl http://x500.pwr.wroc.pl:8888	Wrocław
http://x500.man.poznan.pl:8887	Poznań
http://netman.task.gda.pl:8888	Gdańsk
http://x500.icm.edu.pl:8888	Warszawa
http://lfs.cyf-kr.edu.pl:8888	Kraków

7. Literatura

1. Data Networks and Open System Communications: *Directory*, ITU-T Recommendations X.500-X.525
2. David Chadwick, *„Understanding X.500 Directory"*, 1994
3. Raporty i prace na temat projektu X.500 w Polsce
   http://ocelot.uni.torun.pl/raporty_pl.html